

**PERFORMANCE WORK STATEMENT (PWS)  
FOR  
THEATER MISSION COMMAND CONTRACT (TMCC) II**

**1.0 INTRODUCTION**

The Headquarters United States Army Europe (USAREUR) is the Army component of the European Combatant Command (EUCOM). USAREUR and its assigned forces operate Command, Control, Communication, Computer, and Intelligence (C4I) systems. USAREUR requires Contractor Information Technology (IT) services for sustainment support in garrison and deployed locations to operate, maintain, design and engineer, develop, deploy, integrate, test, train, and perform software configuration of Mission Command Networks and Systems supporting USAREUR, Joint, Coalition, and North Atlantic Treaty Organization (NATO) operations. Within HQ USAREUR, the G3 is the principle staff proponent for planning, task organization, training, orders and Command and Control (C2) mechanisms to commit Army forces in Europe to missions assigned by the Commanding General, USAREUR and the National Command Authority.

**1.1 BACKGROUND**

USAREUR is in the midst of a significant transformational process to reshape its structure and capabilities for combined Multinational coalition forces, North Atlantic Treaty Organizations (NATO) and joint operations within the spectrum of conflict. The USAREUR land component must execute assigned tasks under US Title X to plan, organize, train, equip, and then commit forces per Combatant Command (COCOM) directives. The execution of C4I and C2 responsibilities are performed through Mission Command Networks and Systems utilized by USAREUR within the Joint Information Enterprise (JIE) network. In addition to standard Army-wide Mission Command Networks and Systems, USAREUR has developed applications and systems to meet theater unique requirements to bridge shortcomings in Army-wide systems, interoperability with Joint or Service systems and or integration with Multinational coalition, NATO or with other US Forces.

**1.2 SCOPE**

The purpose of this task order is to provide IT services to support HQ USAREUR, associated staff elements, Direct Reporting Units (as outlined in AR 10-87 Army Commands, Army Service Component Command, and Direct Reporting Units), Generating Force Units, US NATO forces, legacy organizations (AFRICOM J1 J8, AFRICOM CoS, AFRICOM J2 IKD, EUCOM SGS) and other forward deployed DoD organizations and Regionally Aligned Forces (RAF) as part of the overall USAREUR generating forces within the USAREUR Area of Responsibility (AOR).

USAREUR requires IT support services for the continued enhancement, operation, maintenance, and life-cycle support for software and systems applications supporting Mission Command Networks, Systems, and operations. Deployment in support of contingency operations, and other unplanned/unpredictable mission requirements, is required under this task order. This may include deployment to hazardous duty areas, in which it is anticipated that the Government would provide a minimum of 72 hours advanced notice of a deployment requirement. There Government will give as much advanced notice as possible.

USAREUR requires the following capabilities to support this requirement:

- System Availability and Responsiveness
- IT Service Management
- Information Assurance

- Data Protection
- Security
- Adaptability
- Collaboration
- Cross-Domain Security and Information Exchange
- System Interoperability
- Redundancy
- Survivability

The Contractor shall provide IT support services in the areas defined within this document including Mission Command Networks and Systems. This support will be provided to various USAREUR, subordinate organizations and forward deployed DoD organizations across multiple sites and to locations around the world as required.

The Contractor shall provide the requisite number of technically qualified and technically accredited and approved expert support service employees with appropriate security clearances to perform the work described in this PWS.

The Contractor shall follow and apply industry best practices and standards to the maximum extent possible. Contractor personnel shall have an understanding of these best practices and standards as appropriate for their specialized areas. The contractor is responsible for ensuring that their staff is well trained on current technologies and on industry best practices.

### **1.3 TECHNOLOGY FORECAST SUPPORT**

It is required that the contractor maintain technical skills to enable support for the logical progression and industry solutions for hardware and software used at the mission sites. Within 90 days of the contract award, the mission owners will provide a forecast of expected technology evolution to enable the contractor to plan for mission support.

## **2.0 APPLICABLE DOCUMENTS**

The contractor shall comply with the "Mandatory" publications and Army regulations below, and publications are considered part of this task order. The Contractor shall use current commercial practices and current publications whenever possible. The PWS may set a higher standard of performance than an applicable Army regulation, and the PWS will have precedence over the regulations unless a particular PWS provision is in direct conflict with the applicable provision of the Army regulation. Unless otherwise noted, the publications can be accessed at [www.apd.army.mil](http://www.apd.army.mil) and [www.aepubs.army.mil](http://www.aepubs.army.mil). Upon request, the Government will provide those publications not available on a web site. The Contractor shall comply with all changes to the publications, and shall inform the CO of any changes to a publication or document that impact the cost of the task order. Additional technical design and policy reference information governing the SIPRNET can be accessed at: <http://iase.disa.mil/policy-guidance/index.html#trustedproducts> and <http://iase.disa.mil/stigs/iadocs.html>.

### **2.1 GOVERNMENT DOCUMENTS**

- AE Pamphlet 25-1 USAREUR Information Systems Architecture, 11 Jul 2002
- AER 10-5, Organization and Responsibilities, 11 November 2007
- DFARS 252.242-7003, Application for U.S. Government Shipping Documentation /Instructions (Dec 1991)
- AER 25-2, Army in Europe Information Assurance, 18 October 2012

- AER 190-16 – Installation Access Control
- AER 380-40 Safeguarding and Controlling Communications Security Material
- AER 525-13 Antiterrorism/Operations, 30 Mar 2009
- AER 600-700 Theater Expert Accreditation Status
- AE SUPPLEMENT 1 to AR 25-1 Army Information Management, 18 Sep 2002
- AE 600-702
- AR 10-87 Army Commands, Army Service Component Command, and Direct Reporting Units
- AR 25-1, Army Knowledge Management and Information Technology, 2 July 2005
- AR 25-2, Information Management Information Assurance, Rapid Action Revision (RAR) Issue Date: 23 March 2009
- AR 380-40, Safeguarding and Controlling Communications Security Material, 09 July 2012, Rapid Action Revision (RAR) Issue Date: 24 April 2013
- AR 380-5, Department of the Army Information Security Program, 29 Sept 2000
- AR 381-12 Military Intelligence Threat Awareness and Reporting Program, 4 Oct 2010
- AR 715-9, Operational Contract Support Planning and Management, 20 June 2011
- DA PAM 700-31, Commander's Handbook for Peacekeeping Operations, 1 Jul 1994
- DA Pamphlet 715-16, Contractor Deployment Guide, 25 Feb 1998
- DD Form 254 Contract Security Classification Specification
- Directive-Type Memorandum (DTM) 09-012, "Interim Policy Guidance for DoD Physical Access Control requirements is the Installation Access Control System (IACS)
- DoD Instruction, Contractor Personnel Authorized to Accompany the U.S. Armed Forces, October 3, 2005
- DOD 5200.08-R – Physical Security Program, DoD Instruction 5200.08 – Security of DoD Installations and Resources
- DoD 5220.22-M: National Industrial Security Program Operating Manual, 7 April 2006
- DoD 8510.1 -M, DOD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual, July 2000 DoD Directive 8570.01, Information Assurance Training, Certification, and Workforce Management, Certified Current as of April 23, 2007
- DoD DIR-8000.1 Management of DoDDoD Information Resources and Information Technology, 27 Feb. 2002
- DoD Directive 5200.28: Security Requirements for Automated Information Systems (AISs), March 21, 1988
- DoD Joint Information Environment EXORD (AMHS 3.1.3 12.12.0.36), DTG 051530z Dec 12
- DoD Instruction 3020.41 , "Contractor Personnel Authorized to Accompany the U.S. Armed Forces," October 3, 2005
- DoD Manual 8570.01-M, Information Assurance Workforce Improvement Program. Incorporating Change 3, January 24, 2012.
- DOD I 8510.01, Risk Management Framework (RMF) for DoD Information Technology, March 12, 2014.
- FM 3-100.21, Contractors on the Battlefield, 26 Mar 2000
- FM 4-100.2, Contracting Support on the Battlefield, 4 Aug 1999
- Joint Publication 4-0, Doctrine for Logistic Support of Joint Operations, Chapter V, Contractors in Theater, Apr 2000
- NATO Status of Forces Agreement (Article 73), and Ambassadorial exchange of Notes, 27 March 98 (can be accessed at <http://www.chrma.hqusareur.army.mil>)
- Public Law 100-235: Computer Security Act of 1987, January 8, 1988

## 2.2 NON-GOVERNMENT DOCUMENTS

- A Guide to the Project Management Body of Knowledge (PMBOK® Guide), Project Management Institute (PMI), latest edition
- Government Extension to the PMBOK® Guide Third Edition, PMI, September 2006
- IT Service Management, Information Technology Infrastructure Library V3, (<http://www.itil-officialsite.com/home/home.asp>)
- Electronic Industries Association (EIA)/ Institute of Electrical and Electronics Engineers (IEEE) J-STD-016-1995 Standard for Information Technology Software Life Cycle Processes, Software Development Acquirer-Supplier Agreement
- IEEE/EIA 12207.0-1996, Software Life Cycle Processes, 2 Mar 1998
- IEEE STD 1219-1993, IEEE Standard for Software Maintenance, 2 June 1993
- Warranty information (Government owned software and hardware)

## 3.0 PLACE OF PERFORMANCE

Performance of this contract could be affected by rebasing, re-stationing and base closures. The level of support required under this contract will be difficult to predict long-term due to currently unknown or unpublished unit and headquarters realignments and deactivations. As the transformation plans are announced, government directed changes in the location(s) where the Contractor is performing may be necessary, and the transformation may cause increases or reductions in the contractor support required to meet USAREUR needs. Additionally, based on Department of Defense (DOD) and Department of Army (DA) taskings and world events, requirements at new support sites, or in support of contingency operations is possible.

Known sites included as part of HQ USAREUR's current baseline are listed below. Performance may be required at all of the sites listed. APPENDIX A provides an additional breakdown of performance locations by unit. The Government reserves the unilateral right to change where work is performed or add additional sites under this task order as necessary to support the USAREUR mission. Current locations include but are not limited to:

- US Army Garrison (USAG) Wiesbaden, Germany
- USAG Rheinland Pfalz, Germany
- USAG Bavaria, Germany
- USAG Stuttgart, Germany
- USAG Benelux, Belgium, Netherlands
- USAG Vicenza, Italy
- Area Support Team (AST), Balkans
- AST Black Sea, Romania, Bulgaria, Ukraine
- RAF locations in Poland, Estonia, Latvia and Lithuania.
- USARAF Theater – Locations throughout the USAFRICOM AOR and deployed locations to include but not limited to Germany, Italy.
- Additional site(s) and number of support personnel included in the user base is anticipated to grow during the period of performance of this task order.

End-user support must be co-located in proximity to the customer base to provide timely support to user needs. The Government may require temporary duty (travel), remote support, exercise or deployment support at other locations cited in APPENDIX A. In addition, deployment of contractor personnel may be required during performance of this task order. It is impossible to predict in advance required locations for future deployments.

## 3.1 GOVERNMENT DIRECTED CHANGE OF DUTY STATION

The Government will provide notice in writing for any required change of duty station, which may be a result of, but not limited to, a base realignment. The contractor shall provide an invoice supported by itemized receipts for any direct moving costs incurred as a result of a government required change of duty station. Reimbursement by the government will not be authorized when the new duty station lies within the government designated daily commuting distance.

#### **4.0 PROGRAM MANAGEMENT**

The Contractor shall provide management and oversight of all activities performed by Contractor personnel, including subcontractors, to meet the requirements identified in this PWS. Specific Program Management Support requirements are detailed in Section 4.1, Program Management Support.

##### **4.1 PROGRAM MANAGEMENT SUPPORT**

The Contractor shall provide program management support under this Task Order utilizing industry best project management practices (Project Management Body of Knowledge (PMBOK®) Guide), which include all of the tasks required to initiate, plan, manage, control, report and close-out this task order. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors/teaming partners, to satisfy the requirements identified in this Performance Work Statement (PWS). The Contractor shall identify a Program Manager (PM) by name, who shall provide management, direction, administration, quality assurance, and leadership of the execution of this Task Order. The Contractor shall identify Contractor Site Leads and/or Technical Leads by name, who shall, in concert with the Contractor's PM, provide day-to-day operational level leadership and technical guidance to contractor personnel performing work under this Task Order.

The Contractor shall participate in integrated project teams and develop project plans, WBS, activity schedules, GANTT charts, Pareto diagrams, PERT charts, and project status reports utilizing standard software tools adopted by USAREUR such as Microsoft Office Suite (Project, Word, Power-Point, etc).

The Contractor shall provide established planning criteria to control, lead, organize, plan, maintain, and set performance standards for the tasks associated with this effort. The Contractor shall implement measures for controlling costs and shall implement reporting and quality control measures to effectively manage this TO (See PWS Section 8.0 for Deliverables requirements).

The Contractor shall document their approach in a Project Management Plan (PMP). The initial draft PMP shall be submitted iaw the Deliverables Schedule in Section 8.0. The PMP shall describe the Contractor's management approach, operating procedures, support priorities, service levels, and estimated staffing. The PMP shall include an overall WBS and associated responsibilities and partnerships between Government organizations. The PMP shall show milestones and tasks for short term and long term projects. The PMP shall, at a minimum, address:

- Process management and control (i.e. monitoring mechanisms, program metrics)
- Personnel management to include coverage and organizational structure
- Financial management to include cost containment and cost forecasting
- Technical Effectiveness to include routine Operation and Maintenance (O&M) and implementation and integration of new hardware and software, and technical refresh procedures
- Operational effectiveness to include system administration, account management, implementation of new hardware and software, and technical refresh procedures
- Quality Control Plan (QCP)
- Quality Assurance Plan (QAP)

- Risk Management Plan (RMP)
- The PMP shall include establishment of task support in relation to incrementally provided funding IAW customer established task priorities. The PMP shall document prioritization of support to be performed, level of service, and estimated staffing

The Contractor shall provide the Government with a draft PMP, on which the Government will make comment. The final PMP shall incorporate Government comments. The Contractor shall keep the PMP up-to-date, shall ensure it is accessible electronically at any time, and shall be prepared to brief any PMP content to the Government on 24 hours notice.

The Contractor PM shall review the PMP with the COR on a monthly basis.

#### **4.1.1 SITE SPECIFIC PROGRAM MANAGEMENT PLAN (PMP)**

The Contractor shall document and maintain an up-to-date Program Management Plan (PMP) for each mission owner supported under the contract. The Contractor shall submit the PMP within 30 calendar days of the effective date of the Task Order. The PMP shall describe the proposed management approach. The PMP shall detail Standard Operating Procedures (SOPs) for all tasks. The PMP shall include milestones, tasks, and subtasks required in this Task Order. The PMP shall provide for an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between Government organizations. The PMP shall include the Contractor's Quality Control Plan (QCP), Quality Assurance Plan (QAP), Risk Management Plan (RMP) as well as communications and change management processes to be followed. The PMP shall include, but not be limited to, Process Management and Control (to include monitoring mechanisms, i.e. Program Metrics, and Response to Customer Needs), Personnel Management (to include coverage and organizational structure), Financial Management (to include cost containment and cost forecasting), and Technical Effectiveness (to include routine Operation and Maintenance, and implementation and integration of new hardware and software, and technical refresh procedures).

The Contractor shall ensure the PMP is accessible electronically and shall be prepared to brief PMP content to the Government on 24 hours notice.

The PMP shall include establishment of task support in relation to incrementally provided funding i.a.w. customer established task priorities. The PMP shall document prioritization of support to be performed, level of service, and estimated staffing. The Contractor PM will review the PMP with the COR and customer Client Representative (CR) on a monthly basis.

#### **4.1.2 PROJECT ENGINEERING PLAN**

The Contractor shall provide a monthly Project Engineering Plan (PEP) for managing the backlog of project requests. The monthly Project Engineering Plan shall include status of short term and long term projects.

#### **4.1.3 CONTRACT ACTIVITY AND STATUS MEETINGS**

The Contractor Program Manager shall convene a weekly Contract Activity and Status Meeting with the government Program Manager and/or COR. The scheduling for the Contract Activity and Status Meeting will be at a date and time mutually agreeable to the Contractor and the PM/COR. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activity and status report, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The Contractor shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR within five calendar days following the meeting.



The Contractor shall provide the Government real-time access to metrics on communications and information technology support, to include actual statistics, trend analysis and performance measurements and assessments.

#### **4.1.4 MONTHLY STATUS REPORT (MSR)**

The Contractor shall develop and provide a MSR using common office productivity suite applications, by the 15th of each month via electronic mail to the COR. Information included in the MSR shall be segregated in accordance with a Government approved format. The MSR shall include the following:

- Activities during reporting period, by task (Include: On-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
- Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
- Personnel gains, losses and status (security clearance, TESA, etc.).
- Government actions required.
- Schedule (Shows major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
- Summary of Ad-hoc Technical Reports provided.
- Summary of trips taken, conferences attended, etc. Attach trip reports to the MSR for reporting period.
- Accumulated invoiced cost for each CLIN up to the previous month.
- Projected cost of each CLIN for the current month and forecasts through the end of the current performance period.
- Comparison data / monthly performance reports.

#### **4.1.5 PROGRAM METRICS**

The Contractor shall provide the Government with written Monthly Metrics which:

- Provide quantitative measurements which capture and evaluate communications and information technology support, identify trends, and measure performance.
- Serve as a measure of contractor effectiveness.

The Contractor shall work with the Government to identify and incorporate specific measures to include: establishing specific measures; methods of calculation and manner of collection; and the format for reporting.

#### **4.1.6 TRIP REPORTS**

The Government will identify the need for a Trip Report (if required) when the request for travel is submitted to the COR. The Contractor shall keep a summary of all long-distance travel, to include, at a minimum, the name of the employee, purpose of trip, location of travel, duration of trip, and POC at travel location.

#### **4.2 KICK-OFF MEETING**

The Contractor shall schedule, coordinate, and conduct a Kick-Off Meeting through the COR at a location approved by the Government within five (5) business days of Task Order Award (TOA). The meeting will provide an introduction between the Contractor personnel and Government personnel who will be involved with the task order. The meeting will provide the opportunity to discuss transition, technical, management, security, administrative, travel authorization, reporting, and invoicing procedures. At a minimum, the attendees shall include key Contractor personnel, representatives from the directorates, other key Government personnel, and representatives of the Contracting Activity. The Contractor shall provide the following at the kickoff meeting:

- Transition Plan

- Technical Expert Status Accreditation (TESA) Documentation (See 4.4)
- Quality Control Plan

#### **4.3 TRANSITION-IN**

The Task Order transition-in and ramp-up period is expected to begin from date of award and will be phase-in with full performance for all sites beginning NLT 4 April 2016. The transition plan shall be delivered NLT the scheduled contract kick-off meeting. The Contractor shall begin transition-in activities immediately after task order award.

The Contractor shall perform the following activities during the transition-in period:

- Provide a transition-in Plan Of Action and Milestone (POA&M) schedule to the Government.
- Perform joint inventories and inspections of all furnished facilities and property with the government and outgoing Contractor.
- Perform joint identification and inventory of all Contractor maintained equipment, software, and stock relevant to the performance of the contract.
- Perform joint identification and inventory of all Contractor maintained classified data, if any to ensure that proper accountability and chain of custody is maintained.
- Develop and validate a comprehensive baseline for the supported equipment list with the Government and outgoing Contractor.
- Coordinate with the Government to validate or establish maintenance priorities for supported equipment.
- Establish procedures with the outgoing Contractor to transition operations, maintenance, and logistics functions without degradation of service. This includes defining processes for turn-over of system administration, accounts, privileges, and accesses.
- Accept Government Furnished Information (GFI) such as smartbooks, Standard Operating Procedures (SOP), Conunity Of Operations (CONOPS), Techniques, Tactics, and Procedures (TTP), and other technical documentation from outgoing Contractor.
- Accept project management documentation from outgoing Contractor.

Associate Contractor Considerations: There are functions within the scope of this task order where the Contractor must cooperate, share information, or otherwise jointly collaborate in the accomplishment of the Government's requirements with other Contractors working on separate Government contracts. Where such Contractor-to-Contractor interfaces arise, the Contractor shall establish professional relationships with associate Contractors to ensure the greatest degree of cooperation in sharing information, data, technical knowledge, expertise, or resources essential to successfully support the respective missions for USAREUR and the organizations supported under this task order.

#### **4.4 TECHNICAL EXPERT STATUS ACCREDITATION (TESA) and INDIVIDUAL LOGISTICAL SUPPORT**

The Contractor shall comply with DOD Contractor Personnel Office (DOCPer) TESA requirements. DOCPer information and resources can be obtained at <http://www.per.hqusareur.army.mil/cpd/docper/default.htm>. Upon successful TESA application approval, the contract employee will receive Individual Logistic Support (ILS). The current ILS privileges can be obtained at: <http://www.eur.army.mil/g1/content/CPD/docper/ILSvalues.html>. Appendix B provides a list of ILS privileges as of September 2015.

The Contractor shall submit TESA applications using the DOCPer Contractor Online Processing System (DCOPS). The Contractor shall name an individual located in Germany who is designated in DCOPS as the party responsible



for managing and administering the TESA process. The Contractor's designated representative shall work with the COR to complete Phase I and II approvals and shall ensure continued compliance with TESA requirements throughout performance.

At the Kick-Off Meeting, the Contractor shall submit documentation necessary for TESA Phase I Contract Approval to the COR, including but not limited to:

- A copy of all subcontractor agreements;
- All applicable TESA job descriptions;
- First and last name of Contractor's designated TESA representative located in Germany with email address, phone number, fax number, address, city, country, postal code, etc.

Upon receiving Phase I approval, the Contractor shall submit completed, TESA Phase II Individual Applicant documentation to the COR through DCOPS, including but not limited to applications, resumes, employee employment contracts, and supporting documentation. After review and approval the COR will submit TESA documents through DOCPER for approval and routing to applicable authorities.

The Contractor shall assist the COR in complying with AE Reg 715-9(4)(d) by:

- Ensuring TESA application packages are accurate and complete and that applicants meet approved job requirements;
- Providing timely notification to the COR when staffing changes and employee terminations occur which in turn will allow the COR to inform DOCPER and IMCOM-E of such terminations
- Facilitating Turn-in of contractor Common Access Cards (CACs) and identification (ID) cards to local ID-card facilities after terminations.

NOTE: Individual Logistical Support will only be provided to TESA approved employees.

#### **4.5 TRANSITION OUT**

Prior to expiration of this task order, the Contractor shall provide a written Transition-Out plan NLT 180 days, or earlier if directed by the Government. The Transition-Out plan shall facilitate the accomplishment of a seamless transition from the incumbent to incoming Contractor and/or Government personnel at the expiration of the task order. Within the plan, the Contractor shall identify how it will coordinate with the incoming Contractor and Government personnel to transfer knowledge regarding the following:

- Project management processes
- Points of contact
- Location of technical and project management documentation
- Status of ongoing technical initiatives
- Technical artifacts and configuration baselines
- Transfer of portal data
- Appropriate Contractor-to-Contractor coordination to ensure a seamless transition
- Transition of personnel
- Identify schedules and milestones
- Identify actions required of the Government
- Establish and maintain effective communication with the incoming Contractor/Government personnel for the period of the transition
- Inventory of assets and transfer of government furnished equipment, i.e. software and hardware, licenses, warranties, etc.

- System administration, accounts, privileges, and accesses
- Existing leases and rental contracts, if any
- Delivery of Government Furnished Information (GFI) such as smartbooks, Standard Operating Procedures (SOP), Continuity Of Operations (CONOPS), Techniques, Tactics, and Procedures (TTP), and other technical documentation to Government or in-coming Contractor

## **5.0 CONTRACT SERVICES/DISCIPLINES**

### **5.1 ON-SITE PRESENCE**

The Contractor's designated point(s) of contact must be able to triage the reported outage and contact on-call personnel when required. All contractor personnel shall report to duty at the designated Government site. It is expected that the on-site POC will be able to perform normal duties as assigned. The contractor shall appoint a lead for each site for communication purposes.

### **5.2 ON-CALL SUPPORT**

The Contractor shall provide on-call support for exceptional or emergency requirements which occur outside of normal duty hours when requested. Exceptional or emergency requirements are defined as:

- All Maintenance Priority 1 and 2 outages inclusive of VIP end user devices
- All Maintenance Priority 3 outages involving systems, network equipment, and VTC suites but not inclusive of non-VIP individual end user outages.

*Note: Very Important Person (VIP) - VIPs include end users in key leadership and management positions with enhanced service desk and desk side support service requirements. The VIP minimum standard is a Military Grade O-6 or above (or the Civilian equivalent). VIP personnel will be named on a case by case basis from the USAREUR G6 HSD.*

The Contractor shall establish procedures (to include on-call rosters) for each supported site. The Contractor shall respond telephonically to an outage with a technician qualified in the required service area within:

- 1 hour of notification for all locations.

The Contractor shall respond on-site with a technician qualified in the required service area within:

- 2 hours of initial notification should the outage remain unresolved - for all locations.

On-site troubleshooting shall continue for as long as the outage remains unresolved. Travel time to and from the work site is not a billable expense.

*Note: On-duty personnel may provide initial response however should the outage/problem remain unresolved they shall notify the on-call designated subject matter technician within the aforementioned time periods.*

### **5.3 OPERATIONS AND EXERCISE SUPPORT**

The Contractor shall participate, when directed, in operations and exercises, consistent with the level of service specified by the Government's technical direction.

Operations are typically unannounced and have an unknown duration. The Contractor may be required to surge current work force to meet 24x7 operation needs. As much as possible this surge should be satisfied within existing staffing levels and without degradation of service. However, if needed, the Contractor may request

overtime and/or relief from service levels from the Government. Should operations continue long enough, the Government may require, or the Contractor may request additional resource be brought in TDY to meet mission needs.

Exercises are planned events; therefore, although additional work may be required, there should be sufficient time to schedule the work to not impact current operations. Normally exercise scenarios progress on a non-mission interference basis during normal duty hours. The Contractor shall coordinate with the Government to adjust staff schedules to support exercises while concurrently delivering ongoing day-to-day services and support within the available staffing levels. Where directed by the Government, the Contractor shall provide 24x7 coverage during the exercises. This may include adjusting the normal work schedule or minimizing/prohibiting leave of individual contractor employees to achieve the required coverage.

The scope of operations and exercise support includes, but is not limited to:

- Configuring and deploying hardware to support the operation/exercise
- Establishing new or expanding existing network services
- Establishing new or expanding existing Operation Centers
- Troubleshooting and resolving network and user problems

Requirements for providing operations/exercise support include providing support for Program Managed Tactical Communications and or Systems. Travel may be required and while these sites may be austere, the Contractor shall not be required to deploy (travel) under field conditions.

*Note: Requirements described in this section are applicable to networks, services, and systems supported and described in the various attachments. Other Operation/Exercise support may be deemed in scope, but may be accomplished by exercising a unilateral optional requirement from PWS section 6.OPT.*

The Contractor shall not increase manpower or man-hours for Operations or Exercise participation unless authorized by the Contracting Officer (CO)).

#### **5.4 SYSTEM ADMINISTRATION AND MAINTENANCE SERVICES**

The Contractor shall provide continuous system administration services. System Administration services consist of common system administration tasks, system security tasks, and system capacity planning tasks.

##### **COMMON SYSTEM ADMINISTRATION TASKS**

The Contractor shall perform the following common system administration tasks on physical and virtual server platforms:

- Analyzing system logs and identifying potential issues with computer systems
- Introducing and integrating new technologies into existing data center environments
- Performing routine audits of systems and software
- Performing backups and data recovery
- Applying operating system updates, patches, and configuration changes
- Installing and configuring new hardware and software
- Adding, removing, or updating user account information
- Answering technical queries and assisting users
- Responsibility for documenting the configuration of the system
- Troubleshooting any reported problems
- System performance tuning

- Configure, Add, Delete File Systems

### **SYSTEM MAINTENANCE TASKS**

The Contractor shall provide and perform maintenance when directed for communications and IT network systems, and devices, to include, but not limited to, the NIPRNet, SIPRNet, coalition, command and control, and other supported networks and systems, inclusive of:

- Windows-based, Oracle Solaris UNIX-based servers, and LINUX-based servers
- Windows-based, Oracle Solaris UNIX-based, and MAC-based workstations, laptops, or tablets
- Thin clients/zero client terminals
- Video teleconferencing equipment
- LAN hardware including hubs, routers, and switches

Maintenance Priority 1 – CRITICAL – is assigned to:

- Outages of all MAC I systems and equipment
- Outages of systems and equipment supporting identified VIPs to include office, home, and mobile locations
- Outages deemed critical by personnel authorized to give technical direction to the contractor under this contract

Maintenance Priority 2 – URGENT – is assigned to:

- Outages of MAC II systems and equipment affecting more than 25% of users
- Outages of MAC II systems and network equipment supporting local/national emergencies
- Outages of equipment and systems supporting all other VIPs not defined in Priority 1 to include office, home, and mobile locations
- Outages deemed serious by personnel authorized to give technical direction to the contractor under this contract

Maintenance Priority 3 – HIGH – is assigned to:

- Outages of MAC II systems and network equipment affecting less than 25% of users
- Outages of MAC III equipment and systems more than 10% of users
- Outages of bridge-type (conference room) VTC suites
- Individual end user outages rendering assigned desktop/laptop workstation inoperative
- Outages deemed a priority by personnel authorized to give technical direction to the contractor under this contract

Maintenance Priority 4 – ROUTINE – is assigned to:

- Outages of MAC III systems and network equipment affecting less than 10% of users
- All end user outages not otherwise defined
- All scheduled maintenance that do not meet the definitions of Maintenance Priorities 1 – 3

### **SYSTEM SECURITY TASKS**

The Contractor shall perform the following system security tasks:

- Maintain all system devices (servers) i.a.w. USAREUR Information Assurance Program Management, Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS) and CYBERCOM taskings.

- Take appropriate measures to respond to known and possible network attacks i.a.w. applicable DoD policies, directives and instructions, or as directed by the CND Service provider.
- Ensure all Contractor managed items are configured to store and archive all system, device, application, and security event logs i.a.w. DOD and (if applicable) NATO security policies.
- Auditing and reviewing all system, device, application, and security event logs i.a.w. DOD and (if applicable) NATO security policy.
- Reporting, mitigating and/or resolving all classified security incidents (e.g. data spills) that impact networks within time constraints identified by the applicable directive or as directed by the Computer Network Defense (CND) Service Provider.
- Supporting incident reporting activities i.a.w. CND Service Provider and USAREUR policies.
- Supporting and providing the necessary information (i.e. firewall logs, system logs, storage media, etc.) to the USAREUR G6 IAPM and other government designated organizations in the performance of forensic analysis services.

#### **SYSTEM STORAGE CAPACITY PLANNING**

The Contractor shall assist the Government in identifying and matching the storage needs of Contractor operated and maintained systems to allocated storage space. The Contractor shall perform assessments as to whether there are potential problems and issues that must be addressed, and provide the results to the Government. The Contractor shall provide the following storage capacity related services:

- Follow the Backup and Recovery plans to ensure there is no application performance degradation according to service-level agreements
- Manage allocated storage to avoid incidents caused by lack of capacity
- Justify and request additional storage should it become necessary

#### **CONTINUITY OF OPERATIONS (COO)**

The Contractor shall provide for the operation and support of the Government designated COOP sites in the event current services/facilities are inoperable and will remain so for an undetermined amount of time. Enclave boundary defense and security measures at the COOP site must be equivalent to the primary site. The Contractor shall provide analyses, engineering assessments, preliminary studies, and recommendations to assist in the IT portion of the current COOP plan as well as establishing and fielding their next-generation COOP capability.

#### **COO PLAN (COOP)**

The Government's requirement is to exercise and report DRP and COOP on at least an annual basis. The Contractor shall participate in COOP exercises on a regular basis as directed by the Government to ensure complete functionality as defined by the plans. The Contractor shall develop and provide the Government with a specific COOP exercise plan based upon stated Government requirements and objectives for each exercise at least 30 calendar days prior to the anticipated start date of the exercise. Post exercise, the Contractor shall provide an assessment of the exercise. The Government is responsible for maintaining the COOP plan, and the contractor is responsible to assist in the COOP execution.

The Government's requirement is to maintain a hard copy of the DRP and COOP at the primary and alternate site. Alternate site maintenance shall be as specified by the Government.

#### **5.5 PORTAL SERVICES (SharePoint)**

The Contractor shall provide the required support necessary to ensure optimal operation for the mission owner. This support includes, but is not limited to, administration, integration, and troubleshooting all aspects of the Portal and associated software applications and services. The Contractor shall possess the knowledge to install

additional enhancement features to the Portal (such as advanced web parts), build templates, write stored procedures, perform basic database maintenance, and deploy features. The Contractor shall administer, maintain, and back-up SharePoint user pages and associated SQL databases for all activities. This task includes the provisioning and refinement of the SharePoint design, permissions, and possible data migration from an existing site to a new location. The contractor shall:

- Upgrade and migrate to future releases of SharePoint and SQL databases as directed.
- Provide communications and IT O&M support for hardware and software identified by the Government as necessary for portal capabilities.
- Install, configure, and troubleshoot the production system and associated applications in all environments.
- Perform system administration, domain administration, network administration and Lab engineering & administration.
- Support OS/Virtualization and other unique services which include ADFS, Integration, REL, and Identity Management.
- Maintain system administration and day-to-day operations on the development network.
- Install, integrate, test, and deploy applications i.a.w. approved test plans.
- Partner with application development team to help solve business needs.
- Administer and support infrastructure technologies in the Collaboration and Content Management space to include but not limited to: CRM, BI, OCS/LYNC, MOSS, SharePoint.
- Upgrade the various technologies as required.
- Complete assigned day-to-day support ticket requests for the above technologies.

## **5.6 COLLABORATION SERVICES**

The Contractor shall provide Systems Analysis, Systems Engineering, System Administration, Information Assurance, and end-user support services for Mission Owner Portal(s) which includes primarily web-based tools required for collaboration, planning, and operational support. The Contractor shall perform specific duties that include, but are not limited to:

- Oversee the SharePoint application portfolio on SIPR and NIPR networks;
- Integrate / configure .NET applications and SharePoint technologies with SQL Server database on NIPR and SIPR;
- Maintain the various SQL databases supporting OCS/LYNC, CRM/TMT, and IIS/Web Applications;
- Monitor performance of SharePoint architecture and web based applications after implementation;
- Advise the Content Manager, and the Content Coordinator(s) on proper document profiling and customization for the mission owner Portal (SharePoint);
- Perform SharePoint administration to configure settings that affect the system service, such as load balancing for indexes; to setting priorities for applications;
- Perform stress testing and other operations on the web storage system, the dashboard site, SharePoint servers and web parts, to assure optimal system performance;
- Maintain application documentation to describe software components development, logic, coding, testing, changes, and corrections;
- Assist the Application Development Team in the full lifecycle development of portal applications/parts including functional requirements, analysis, and user interface design, database design, security control setup, testing and documentation;
- Operate and maintain desktop tools to provide end users with the ability to fully utilize the collaboration functionality such as OCS/LYNC.

## **5.7 WEB/MEDIA SERVICES/ADMINISTRATION**



## **WEB/MEDIA SERVICES**

The Contractor shall provide Web design and Web content administrator support to maintain and improve Web-based systems. The scope of services includes planning, designing, testing, and implementing static and dynamic Web pages, Web sites, Web applications and associated content. The Contractor shall deliver production management, Web page design, markup languages, scripting, and relevant web/media services support. WEB/MEDIA service changes to the communications and IT baseline shall be planned and implemented IAW established formal configuration management and change control processes.

## **WEB DESIGN**

The Contractor shall apply knowledge, skills, and user interface design experience to design, develop, and maintain a consistent web information architecture, user interface features, site animation, and special-effects elements that ensure predictable, successful user interactions. Web site designs shall support the organization's strategies and goals relative to external communications. The Contractor shall provide Web design and administration services to mission owner web-based systems. The scope of services include planning, designing, testing, and implementing static and dynamic Web pages, Web sites, Web applications and associated content. The Contractor shall deliver production management, web page design, markup languages, scripting, and relevant web/media services support. WEB/MEDIA service changes to the communications and IT baseline shall be planned and implemented i.a.w. established, formal configuration management and change control processes.

The Contractor shall apply knowledge, skills, and strong user interface design experience, along with web development experience to:

- Provide O&M Tier II support services upon request to assist in problem resolution.
- Ensure web content provided is optimized in a manner that motivates, entertains, educates, engages, and appeals to the user community such that it encourages regular access and use as a major source for information and decision making.
- Produce site-maps, wire-frames, mock-ups (without graphics design), and style-guides.
- Design, develop, and maintain a consistent information architecture, user interface features, site animation, and special-effects elements to ensure predictable, successful user interactions.
- Create scripts/code that interact with web servers, the content for web-based systems, and provides dynamic web content through the web/internet servers.
- Seek user community feedback and input for improving and enhancing web sites.
- Develop and implement standards/guidelines subject to Government approval.
- Advise and coordinate with content developers on requirements, and applicable standards.
- Contribute to the design group's efforts to enhance the look and feel of the online offerings.
- Research and recommend web-technologies with respect to the distribution of content, collaboration, and information sharing.
- Identify and resolve technical issues with web-based systems and content.
- Apply appropriate security measures; provide for the appropriate use of copyrighted material; and produce reports and other documentation.

## **WEB/MEDIA CONTENT ADMINISTRATION**

The contractor shall be responsible for developing and maintaining the baseline for web site information architecture, as well as for designing and developing the content delivered via the web sites. The contractor shall apply knowledge of information design and information architecture, usability, graphic design, communications, and related fields to produce professional quality web content for publication on command web sites. This work includes developing user cases for information delivery, organizing, managing, maintaining, updating, writing, integrating, and editing Web content.

## **5.8 CUSTOMER SUPPORT SERVICES**

The Contractor shall apply a broad base of IT knowledge and subject matter expertise to identify, recommend and properly apply solutions, implement products and deploy baselines and services. In addition, the Contractor shall perform Tier III problem resolution services combining their expertise with the latest technology available to proactively avoid issues and restore degraded IT systems quickly and effectively. Contractor shall provide systems and technical management support for C4I Networks and systems, including the SIPRnet, NIPRNET, COLAN, and JWICS systems. The contractor shall provide:

- Dedicated end user service technicians when specified by the Government
- Respond to user telephonic and electronic requests for assistance
- Extended service hours to support real world operations and exercises
- Desktop support, super user assistance, touch maintenance and hardware/software troubleshooting support for laptops, desktop computer systems, printers, access control and security systems, briefing and VTC systems and other devices
- IT system installation, maintenance and high availability
- Information Assurance and Security Baseline configuration and compliance
- Performance monitoring and overall reliability and effectiveness of CIS and IT services
- Enabling authorized connectivity, operation, or use of available networks, equipment and technologies to meet garrison and deployed operational requirements validated by the Government representative
- Scheduling, initiating, and operating of VTC systems and/or facilities, as requested
- Subject matter expertise for end users upon request for required data services or applications, consistent with requirements and authorizations
- Install, operate, and maintain networked VTC services on SIPRNET, NIPRNET, and JWICS
- Software, system, and network administration and systems sustainment of strategic and tactical video walls, video teleconference suites, and Multipoint Control Units (MCU)

NOTE: At this time, no remote support is authorized.

## **5.9 ACCOUNTS MANAGEMENT AND PUBLIC KEY INFRASTRUCTURE (PKI) TOKEN SERVICES**

The Contractor shall provide a consolidated account management service desk which provisions and de-provisions IT systems accounts as personnel are assigned to or departing from the mission owner AOR. Assigned contractor staffs are required to certify and perform as Enhanced Trusted Agents (ETAs) for SIPR/Alt Token services. Account management services shall include at a minimum:

- Validation of 8570.01 requirements
- Account creation/deletion
- Updating of GAL information
- Issuance and management of User Agreements
- Active Directory integration and Group Policy requirements.

## **TOKEN MANAGEMENT SERVICES**

The Contractor shall provide services to develop/enhance Army processes throughout full life cycle sustainment of the Public Key Infrastructure (PKI) Token Management system. Contractor support activities shall include:

- Process development/enhancements to support the issuance of tokens to military, civilian, and contractors who have Army sponsored accounts
- Travel to Army sites within Europe to gather data for processes development/enhancement

## **Local Registration Authority (LRA)**

The Contractor shall provide personnel trained and certified as an LRA. Training is limited and therefore must be scheduled well in advance; LRA Training consists of a 2-step process (DOD and Army specific) and is only

available in CONUS. Prime performance location is designated as Clay Kaserne, Wiesbaden, Germany. The certified LRA shall support the following LRA functions:

- Sourcing, distribution, and installation of user PKI devices
- Identity proofing of certificate applicants for requestors (end users)
- Using the Token Management System to authorize certificate issuance, certificate suspension, restoration, PIN reset or key recovery
- Authenticating revocation requests and forwarding the requests to an authorized RA
- Unlocking subscriber tokens
- Assisting System Administrators with obtaining server certificates
- Transmitting certificates to ETAs when required
- Managing Enhanced Trusted Agents and Trusted Agents
- Logging and record keeping requirements; and Technical aspects

**\*\*Individuals designated as LRAs do not have the authority to revoke, suspend, restore certificates, or perform key recovery operations**

#### **Registration Authority (RA)**

The Contractor shall provide dedicated personnel trained, certified and appointed by CIO as Registration Authorities. Training is limited therefore must be scheduled well in advance; RA Training consists of a 2-step process (DOD and Army specific) and is only available in CONUS. The certified RAs shall provide all the functions of an LRA and the following RA functions:

- Controls over the registration process as well as the identification and authentication process
- Register / Approve LRA requests
- Approve server certificate requests
- Approve domain controller certificate requests
- Generate mobile code certificates
- Generate alternate logging certificates
- Search CAs for certificate information
- Suspend / Restore subscriber tokens
- Revoke Certificates
- Key Recovery Operations

#### **5.10 COALITION NETWORK END USER SUPPORT**

The Contractor shall provide end user support for various Coalition systems i.a.w. the requirements for communications and IT support. Coalition/Partner Networks are defined as any network that is utilized by the mission owner (i.e. USAREUR) for mission purposes that contains non-DoD endpoints. Typically connectivity is provided via a tunnel through the existing network(s). The contractor shall provide network engineering support as required to initiate and maintain these coalition services in the requested facilities.

The Contractor shall develop a simplified construct that is flexible and can be utilized to service any network utilized. The tiered support structure should be tailored to provide responsive services within each tier to enable effective support to the mission. The scope encompasses base line support covered under this Task Order. The Contractor shall provide:

- I: Touch labor to ensure transport to include tunnel is active and end point has IP services
- II: Tier I plus management of some localized services/servers and desktop support (imaging and touch labor)
- III: Full network that is engineered, designed, O&M'd by the mission owner

Coalition Networks to be supported include but not limited to:

- CENTRIXS
- US BICES
- NATO Secret
- STONEGHOST
- SEAGULL
- TALON
- Future coalition networks.

#### **5.11 VIRTUAL DESKTOP INFRASTRUCTURE (VDI) OPERATION & MAINTENANCE SERVICES**

The Contractor shall provide Operations and Maintenance support to include applicable IA services for USAREUR VDI infrastructure for desktop presentation in single or multi-level security environments. The Contractor shall be responsible for O&M on all servers, storage, applications, and network equipment as identified by the mission owner. O&M services encompass support for the current Phase 1 VDI server environment (as required), VDI Storage Area Network, CITRIX desktop environment as well as user end points connected to the applicable network. These services span other PWS requirements (i.e. system administration, network management, configuration management, information assurance, storage management, etc.) described elsewhere in PWS section 5.0 CONTRACT SERVICES/DISCIPLINES.

#### **5.12 COMMAND AND CONTROL (C2) SYSTEMS & APPLICATIONS SERVICES**

The Contractor shall provide C2 systems applications and services support for the mission owner in the areas of systems engineering; server configuration; software engineering; and display management. This support is limited to what is allowable by Global Command and Control System - Joint (GCCS-J) Program Management Office (PMO). In addition, this PWS is intended to provide O&M services as it relates to IT and not Operator Services (such as Common Operating Picture management).

The Contractor shall provide the following C2 system support:

- Procurement of hardware with minimum specifications as determined by the PMO and GOTS developer
- Proposed device connectivity as determined by the PMO and GOTS developer
- Proposed rack space design for servers with proper cooling systems
- Installation of GOTS and Government-provided equipment and software that is not proprietary and does not require specialized installation
- System Administration; System Maintenance; Technical Refresh/Upgrade Support

#### **5.13 SYSTEM ENGINEERING/ADMINISTRATION AND MIGRATION SERVICES**

The Contractor shall provide System Engineering Support services to improve customer service, system performance, and reliability for the C4 Systems for projects as designated by the mission owner. The mission owner requires a holistic approach to engineering beginning with the planning process. The Contractor shall apply DoD Unified Capabilities objectives and tenets to engineer the mission owner's solution to support efforts to share and distribute information by electronic means. The Contractor shall look beyond the technological requirements to examine the business processes that are driving those needs. The Contractor's engineering approach shall allow for testing prior to delivery, internal quality checks during the engineering phase as well as Quality Assurance during the migration and transition phase, and disaster recovery requirements built into the solutions. Finally, service migration is more than new technology or platforms; it is moving the users to the new service and addressing/overcoming their needs and fears.

The Contractor may or may not have full control of the Engineering projects they are assigned. Depending upon the scope, size, complexity, and Government needs, the Contractor will often be a member of an integrated teams consisting of both Government and other Contractors.

The Contractor shall provide systems engineering, administration and migration services/support for current and emerging Communications and Information Systems (CIS) architectures and technology platforms, Active Directory integration and Group Policy requirements, software engineering, development and integration services and, as required, CIS and technology solutions to optimize the mission owners operations, data and information processing, customer technical support, IT system design, integration, installation, testing, maintenance, administration, operation, high availability, disaster recovery, daily Information Assurance and Security Baseline configuration and compliance, performance monitoring and overall reliability and effectiveness of CIS and IT services capabilities while supporting legacy systems and meeting new requirements to solve issues, provide operations capabilities, meet mandatory policy and tasks, leverage best business practices and take proper actions when incidents, problems and failures occur. The contractor shall maintain, modify, and support only required legacy applications and follow meet Government guidance in the decommissioning of the applications and systems when no longer required, as well as regulations and mandatory policy applicable to the assets, users and operations within the scope of the organization's IT environment, the building's secure facility (SCIF) and multiple security level environment. The Contractor shall be required to apply extensive industry knowledge and subject matter expertise to identify, recommend and properly apply solutions, implement products, deploy baselines and services and formulate Enterprise-wide IT solutions both in Garrison and in a deployed environment. The Contractor shall provide experienced and certified IT Engineers capable of researching, analyzing, recommending and implementing new technologies, e.g. server virtualization and advance data storage and replication; meeting standards, utilizing correct and approved processes, tools and techniques. In addition, the Contractor shall perform Tier III problem resolution services combining their expertise with the latest technology available to proactively avoid issues and restore degraded IT systems quickly and effectively.

The Contractor's engineering processes will span other areas of this PWS. Logistical support areas such as tool purchasing, asset management, and configuration management will be integral to many of the engineering projects. Information Assurance service area of Architecture and Engineering will assure that required security controls are addressed in the solution.

The Contractor shall provide the following engineering and implementation services that include, but are not limited to:

- Provide requirements planning support for C4I Networks and systems, including the SIPRnet, NIPRNET, COLAN, BICES and JWICS systems to include but not limited to strategic and tactical switches, storage inventory, tunnel solutions, firewall administration, VoIP/VoSIP, REM, SIPR/NIPR/JWICS accreditations, communications solutions, DISA/ISAT inspections, server maintenance, clustering, VM Ware, Active Directory management, BMC SAN management, Microsoft Systems Management, COOP facility planning and management, etc.
- Perform Local and Wide area network (LAN/WAN) architecture design, installation, and administration of tactical and simulated LAN/WAN, Unclassified, Classified, and NIPRNET, SIPRNET, JWICS topology. The Contractor shall support operating systems that include, but are not limited to Microsoft Windows, Sun Solaris and UNIX, Administration of Windows 2008 Server OS and Active Directory.
- Assist in the planning for new and evolving C4I systems, develop and/or evaluate plans for the migration of existing functionality to new platforms and architectures, assess performance of existing systems and make recommendations for corrections and enhancements to the CM.

- Conduct strategic planning, research/studies, and evaluations to identify resource requirements, recommended solutions, associated labor level of effort estimates, and timelines/schedules.
- Coordinate with vendors and Government designated SMEs to select appropriate technologies, products and services in order to produce a comprehensive and cohesive architecture.
- Research, analyze, recommend, and implement (once approved) new technologies, products, standards, processes, tools and techniques and provide recommendations and guidance for the design, development, implementation, integration, security and management of approved products and solutions.
- Develop logical, architectural and detailed designs based on technical specifications/requirements and engineering thresholds.
- Produce detailed system documentation including installation instructions, configurations, troubleshooting information and develop bill of materials (BOMs), monitoring specifications and engineering implementation/integration plan (EIP).
- Respond to trouble tickets providing Tier III technical in-depth support for issues, problems and incidents that cannot be resolved at lower service Tiers.
- Serve as Technical Advisors to the Change Advisory Board and working group forums.
- Test and evaluate commercial-off-the-shelf applications, Government-off-the-shelf applications and hardware for integration into the C4 networks
- Ensure compatibility with current baseline, resolving conflicts as they arise
- Apply appropriate security measures (STIGs, IAVMs, Tasking Order Compliance...etc) to lock down the application/hardware
- Develop deployment procedures (i.e. package software, installation instructions...etc)
- Have Information Assurance review and sign-off acceptability prior to deployment
- Test and evaluate IA directed patches for compatibility with the current baseline and resolve any conflicts prior to deployment
- Provide design and engineering support for new network and system implementations and upgrades to include hardware, software, projection systems, video switching hardware, video teleconferencing, and other systems to meet project requirements
- Develop solutions to migrate services from the current environment to the COCOM approved JIE solution
- Provide Project Management using the Project Management Institute's (PMI) framework and following mission owner processes. Project plans shall clearly identify the Contractor's roles and responsibilities.
- At the Government's direction, develop and maintain the project plan to all sub-plans
- Ensure the engineering solution covers all phases of the project plan including removal of the old technology
- Determine training needs and recommend solutions for both the IT service provider and end user
- Engineer, install, operate and maintain a test lab in support of the mission owner C4 networks.
- Provide effective technical solutions to complex problems to include Tier 3 troubleshooting of incidents or problems when requested
- Produce detailed system documentation including installation instructions, configurations, troubleshooting information and develop bill of materials (BOMs), monitoring specifications and engineering implementation/integration plan (EIP).
- Respond to trouble tickets providing Tier III technical in-depth support for issues, problems and incidents that cannot be resolved at lower service Tiers.
- Serve as Technical Advisors to the Change Advisory Board and working group forums.

Specific known systems and requirements are:



- OS/Platforms: Directory Services; PKI, Client and Server Operating Systems
- Unified Communication Engineering: Exchange, LYNC, Blackberry, SMEPED, Mobile Devices
- Storage Infrastructure Engineering: SAN, SQL, Backup, Virtualization
- Management/Monitoring: SCOM, SCCM, SPECTRUM, Imaging, Updates, Deployment, Circuit Status, SolarWinds
- Portal: IIS/TMT/SharePoint/IE
- Situational Awareness: COP, GCCS-J
- Network Engineering: Routing/Switching/Firewalls/VOIP/VPN
  1. Wireless networking (IEEE 802.11, 802.15, 802.20)
- Global Command Control System (GCCS) Administrator
- Application Integration
- Audio Visual Engineering
- Data Architecture Engineering
- Data Base Design and Architecture
- Server Infrastructure Engineering
- System Engineering
- Technical writing
- Antenna, Aerial, Dish & Radom
- Radio and Transceiver (including data, i.e. HPW, PDA184)
- Communications Vaults & Outbuildings
- Conveyances
- Telecommunications (TELECOM): Cellular-based communications (2G/3G/4G; Voice and Data)
- SATCOM: Tactical Satellite, All relevant bands (Ka, Ku, KuSS, C, X)
- Airborne Satellite Systems (KuSS technologies, antennas, modems, etc)
- ISR distribution technologies (UVDS, GBS, etc) and ISR Aircraft platforms
- Frequency Management
  1. Maintaining and updating the Frequency Allocation Chart
  2. Manage all SINCGARS (ACES) requirements.
  3. Submitting Satellite Access Requests (SARs) for tenant units
  4. Building frequency HOPSET/LOADSETs for rotational units
  5. Determines, manages and assigns operational frequencies for joint tactical exercises
  6. Assisting rotational units with internal SAR requests when related to the exercise mission or follow-on deployments.
  7. SIPR and NIPR Access Point (SNAP) requirements
  8. Submit SARs for SNAP satellite terminals for units deploying for training
  9. Submitting Host National Approval (HNA) license requests for specific operating locations at HTA and GTA;
  10. Maintain an updated listing of all approved SNAP HNAs;
  11. Using SPECTRUM 21 submit frequency SFAFs to USAREUR G6 for JMRC OPSGRP deployments to other locations in Germany or in the USEUCOM AOR
  12. Using Host Nation Spectrum Document Online (HNSWD-O) to determine if radio devices have HN spectrum approval.

*Note: The disciplines anticipated may not be all inclusive. Additionally, inclusion of a discipline does not indicate that one FTE (a full man-year) is needed in that area nor on the other hand that one FTE will suffice.*

#### **5.14 CAPABILITIES PLANNING AND REQUIREMENTS ANALYSIS SUPPORT**

The Contractor shall assist the Government by providing forward-thinking technical direction and engineering services for assessing system performance and business needs, planning for new and evolving C4 systems, evaluating proposals for the migration of existing services, and making recommendations for corrections and enhancements to current systems. Contractor planning services shall include providing draft documentation and technical input to documentation for assessments, plans, system implementations and architectures, and engineering designs related to new, evolving, and existing C4 Networks and systems, including the SIPRnet, NIPRNET, COLAN, and JWICS systems.

At the direction of the Government, the Contractor shall conduct and/or participate in strategic planning, studies, and evaluations to provide resource requirements, present recommended solutions, determine labor and tools estimates, and plan/refine schedules. The Contractor's effort shall include:

- Providing technical studies, reviewing plans, evaluating state of the technologies prior to fielding of new releases or systems
- Reviewing C4 plans and policies and providing observations and questions for consolidated responses
- Researching and coordinating technical issues and requirements and drafting new and updated policy governing technical issues
- Providing technical analyses and draft reports of C4 system tests, assessments, and architectures
- Participation in meetings as required by the Government to include attending conferences; technical interchange seminars; interoperability meetings; and other briefings related to integration, migration, and maintenance of C2, coalition, and bi-lateral system architectures
- Perform analysis, provide recommendations, and prepare planning documentation as directed by the Government for approval to transition current services into the JIE
- Planning large-scale systems and projects through vendor comparison and cost studies and provide input to policy level discussions regarding standards and budget constraints
- Developing Project Charter, Scope Document, and Requirements document as need to satisfy project needs
- Determining Life Cycle Replacement (LCR) needs of supported technology based upon industry standards and budget constraints. Develop and submit a semi-annual LCR plan for Government approval

#### **5.15 SOFTWARE ENGINEERING/APPLICATIONS DEVELOPMENT SERVICES**

The Contractor shall provide applications implementation and integration support to research, test, enhance, debug, implement, and integrate software on multiple platforms to include servers, desktops, and mobile devices for the Joint Information Environment (JIE).

**Specialized Experience:** The System Engineer must possess experience as a .NET programmer with experience using Microsoft SQL database servers with a firm understanding of SQL stored procedures and advanced SQL techniques. Must possess the ability to develop complex software solutions to satisfy design objectives; ability to collect and analyze user requirements for implementation of appropriate solutions; and ability to prepare technical documentation. An understanding of the SharePoint object model is highly desired as well as a familiarity with building custom webpart solution. The System Engineer must obtain certification(s) satisfying the Technical Level II requirements in DoD instruction 8570.1.

The Contractor shall troubleshoot problems with software that is already in production to alleviate issues related to software applications (such as SharePoint, Forefront Identity Management, Active Directory, Systems Center Configuration Manager, Task Management Tool, and others). The contractor shall instruct, assign, direct, and check the work of other software developers on the development team, where applicable.

The Contractor shall lead the development of software user manuals for production systems and systems developed by the contractor to support turnover to operations support teams.

The Contractor shall provide rapid, reliable software engineering support to include database support for instantiations of SharePoint, WEB/MEDIA SERVICES, and customized COTS applications, and other legacy software applications. Additionally, the contractor shall restore WEB/MEDIA SERVICES, SharePoint portals, and other Enterprise applications to full productivity, in accordance with their mission critical service level agreement, following loss of services or unplanned outages. Furthermore, the contractor shall ensure the confidentiality, integrity, and availability of information provisioned by the host organization; i.e. access to Enterprise and mission owner centric applications, and servers. The contractor shall maintain, modify, and support customized legacy applications and systems to extend their life, or aid the Government in the decommissioning of the applications and systems when no longer required.

It is important to note that the Contractor shall provide much of the development and maintenance support down to the source-code level. The Contractor shall produce products in accordance with IEEE 12207, DISA STIG's, and other DOD official guidelines on software development. The contractor shall perform the following duties that include but are not limited to:

- Create, update, and maintain the O&M documentation in accordance with changes and additional system requirements identified/implemented.
- Answer questions and support minor modifications ICW IT service providers (Tier-I/II support) to the mission owner's Process Definitions, InfoPath and Web-maker forms, and respond to Change Control Board (CCB) configuration or problem reports on an ad hoc basis.
- Installation, test, and support upgrades of software.
- Enhance the "Post-Validation" sub-process as directed by the Government.
- Model and enhance business processes/links to Government systems.
- Performs analyses and troubleshoots software comprising Mission Critical Collaboration Systems and the Defense Information System Network-Europe.
- Collects requirements and develops software fixes for software programs.
- Devises software work-around solutions to keep programs on schedule and provides recommendations for new or changing requirements for incorporation into existing or planned systems.
- Submits Engineering Change proposals prior to implementation.
- Performs software user and regression tests.
- Perform code developments, modifications, and customization on legacy and future applications.
- Development, implementation, operation and maintenance of commercial and highly customized web applications, built in .NET with related Microsoft SQL databases to include customizations done on Microsoft SharePoint 2007/2010 enterprise platforms.
- Perform high-level web application and database design functions centered on .NET technologies, analyzing intelligence functional requirements and developing design specifications to satisfy intelligence mission requirements.
- Ensures that software design is interoperable, secure, portable, serviceable, and maintainable; has demonstrated effectiveness and reliability; and is highly operational within the parameters of the system. Reviews data requirements, as well as access and response needs, and recommends application platforms and programming languages to best support them.
- Evaluates and recommends available database management system (DBMS) products to best support validated user requirements.

The Contractor shall provide employees proficient and experienced in the the following computer languages:

C++;	C#;	Visual Basic (VB) Visual Studio
ASP/ASP.NET	VB (script)	Java
Powershell	XAML	MCPD: SharePoint Developer 2010 and various versions
MCPD Web/Windows Developer	MCAD:NET	MCSD: Web /SharePoint Applications
Xamarin One Touch	HTML/CSS	Mobile Apps Development
xRM	Python	Ruby
Pearl	Scripting Languages	

The Contractor shall provide employees proficient and experienced in the following but not limited to applications:

#### SHAREPOINT SERVICES

The Contractor shall perform engineering and development services for hardware and software identified by the Government as necessary for the mission owner's portal capabilities. Specifically, the contractor shall perform duties that include, but are not limited to:

- Install, configure, and troubleshoot the production system and associated applications in all environments.
- Ensure compliance with DISA STIG(s) and other DoD IA requirements
- Perform system administration, domain administration, network administration and Lab engineering & administration.
- Support OS/Virtualization, COOP and other unique services which include ADFS, Forefront, Integration, REL, and Identity Management.
- Provide Tier II and III Portal Support services to include daily completion of assigned trouble tickets.
- Install, integrate, and test applications on the development and staging environment.
- Install and deploy approved applications in the production environments.
- Partner with application development teams to help solve business needs.
- Administer and support infrastructure technologies in the Collaboration and Content Management space: to include CRM, xRM, BI, OCS, SharePoint 2007/2010/2013/and future releases.
- Perform system administration, code modifications, and customization on legacy and future Portal applications.
- Upgrade the various technologies as required.

NOTE: MS SharePoint is the current platform being used for collaboration and document management throughout USAREUR.

#### SQL AND DATABASE SUPPORT

The Contractor shall provide SQL and database maintenance support to the legacy and future applications to include, but not limited to the following applications:

266FMS Exchange Rates	IMCOM-E Road Conditions	SSRS Reports (Remedy, SharePoint, etc.))
AE Pubs (Tier III support)	Legacy LNSP (Tier III support)	TFS

AE-ITT	NIPR	TMT 2.0
AE-ITT (Tier III support)	OJA FCJC	TMT 2.0/3.0
Army Europe Publications (AEPUBS)	OJA NATO SOFA	Unrestricted Web
CIE-E	Restricted DMZ	UPDB (Tier III support)
CIE-N	SharePoint 2007 (eur.aep.army.smil.mil)	USAREUR Flight Scheduler
CIE-S	SharePoint 2010 and 2013 (intranet.eur.army.mil)	USAREUR Morale PIN Issuing Resource-Europe (UMPIRE)
FSA	SharePoint 2010 (intranet.eur.army.smil.mil)	USAREUR Personnel DataBase (UPDB)
Future onboarded apps	SIPR	USAREUR Staff Action Tracking System (USATS)
IMCOM-E OPH	SSRS Reports (Remedy, SharePoint, etc.)	VMWare (hosting RCC-E VMWare dbs)

#### 5.16 ENTERPRISE ENGINEERING AND ARCHITECTURE SERVICES

The Contractor shall provide System Engineering services for complex, large-scale, and/or enterprise-type projects. This support shall include:

- Participate in systems engineering planning activities. Provide feedback to both short-range and long-range planning activities to enhance performance and improve efficiency.
- Provide emerging communications and information technology engineering support and technical solutions to improve overall service delivery to include customer support, network, services, proactive system support, etc.
- Develop Cost Benefit Analysis documentation in support of new technology or processes
- Provide design and engineering support for new network and system implementations and upgrades to include hardware, software, projection systems, video switching hardware, video teleconferencing, and other systems to meet project requirements
- Support the Customer's efforts to share and distribute information by electronic means
- Provide effective technical solutions to complex problems to include Tier 3 troubleshooting of incidents or problems when requested

#### ARCHITECTURE SERVICES

The Contractor shall provide the Government high-level architectural expertise and develop architectural products and deliverables in its responsibility to manage current and future operational and exercise architectures for organizations. The contractor shall formulate: transition, integration, implementation, and upgrade the strategy of systems and design infrastructure for intelligence systems used in support of all USAREUR missions. Additionally, the contractor shall develop systems requirements for garrison and deployed operations of USAREUR organizational units, as well as, technical solutions and process engineering to improve analytical and operational efficiency and effectiveness.

The contractor shall advise the feasibility of potential future projects and evaluate and recommend tools, alternatives, and procedures for: upgrading operating systems, enhancing functionality, managing storage, improving reliability, determining interoperability requirements, minimizing system operational

maintenance requirements, and implementing state-of-the-art technical practices for intelligence systems for USAREUR units within the theater. The contractor shall provide, but not limited to transition, integration and upgrade strategies in support of Department of Defense Intelligence Information System (DoDIIS), Joint, Army, Coalition, and National Agency systems and initiatives.

In order to accomplish the aforementioned requirements, the Contractor shall:

- Participate in and assist the customer with operational evaluations of advanced technologies. The contractor advises USAREUR organizations on selection of technical purchases to assimilate emerging technologies and achieve Army Transformation goals.
- Assist in developing standards, processes, and tools to identify and document intelligence architectural shortfalls, resource requirements associated with current and emerging intelligence systems and concepts, and to assess resources required to achieve target architectures and design
- Assist USAREUR organizations in implementing and operating a Knowledge Management (KM) process to improve tools and processes for publishing, disseminating, analyzing, and managing of intelligence information.
- Assist in developing, designing, implementing, and transforming intelligence platforms including the European Foundry Site, European Intelligence Readiness Operations Center (IROC-E), and Multinational Intelligence Readiness Operations Center (MN-IROC).
- Participate in planning, designing, documenting and implementing Exercise Architectures following the Joint Exercise Life Cycle (JELC) process and provide on-site integration and troubleshooting.

#### **5.17 INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION (C&A)**

The contractor shall provide Information Assurance C&A, now known as Cybersecurity Assessments & Authorization (A&A), services iaw Army Regulations and DIACAP or RMF standards as directed by and in accordance with G6 CyberSecurity or other mission owner developed/managed schedules, procedures and iaw DoDI 8510, Army Regulations and DIACAP or RMF standards. The contractor will notify the government within 1 business day of any government actions that will cause delay.

The Contractor shall provide DoD Information Assurance Certification and Accreditation Process (DIACAP) or Risk Management Framework (RMF) services i.a.w. applicable Government directives to include DODI 8510, Army regulations, and USAREUR standards. The Contractor shall develop, maintain, and evaluate accreditation packages for unclassified and classified networks, information systems, protected distribution systems (PDS), and circuit connections as designated by the QAE.

The contractor shall assist assigned clients with the creation, updating, and delivery of the following artifacts related to the G6 CyberSecurity FISMA Customer Support Tracker tool:

- MAC/CL Memo
- System Identification Profile (SIP)
- Topology Diagrams (DCHW, DCSD)
- Data Flow Diagrams (DCFA)
- Hardware List (DCHW)
- Software List (DCSW)
- HBSS Compliant or Waiver
- Foreign National Memo (PEPF)
- Users and privileged users list (ECPA, DCSD, ECLP)

#### **ACA/SCA-V SERVICES**

The contractor shall provide ACA/SCA-V services as directed by and in accordance with the mission owner developed/managed schedules and procedures. Start dates for all ACA efforts are predicated on the supported



Unit will have provided the necessary validation artifacts via the approved system (currently C&A TdB and/or SIPRNET Dump Site and eventually eMASS). The contractor shall coordinate any change in schedule or postponed validation effort with the QAE that could result in a requirement to retest or at least revalidate any previously completed deliverables due to system or network changes.

#### **GOVERNMENT ACTIONS REQUIRED FOR ACA VALIDATION EFFORTS**

- TdB and eMASS Access provided to validators
- Verified that necessary unit personnel will be available to support validation effort.
- Review and provide comments within 1 week of delivery of DRAFT deliverables.

#### **VALIDATION ARTIFACTS**

Government TdB/SIPR Dump Site/eMASS provided validation artifacts complete and available NLT 1 week (or as negotiated) prior:

- Network topology
- DataFlow Diagram
- Hardware List
- Software List
- Privacy Impact Assessment
- Tenant List, or TSP Workbook as required
- HBSS Compliance Waiver (as required)
- MAC/CL Assignment/CIA Assignment

#### **ACA/SCA-V PREPARATION ACTIONS**

- Prepare Certification Testing and Evaluation Risk Reports and artifacts (iaw the DoD Information Assurance Certification and Accreditation Process (DIACAP) or Risk Management Framework (RMF))
- Evaluation Risk Reports
- Findings Reports sheets
- DIACAP/RMF Scorecard/Security Assessment Report (SAR)
- DIACAP/RMF cover page
- Plans of action and milestones (PAO&M) Supplement
- Perform security testing, risk analysis, and verification using authorized audit tools and methods (such as DISA SCAP Compliance Checker, STIG Viewer, ACAS, Nipper, etc)
- Perform networking device security testing (to include firewalls, routers, switches, etc)
- Perform application security testing in accordance with DISA STIGs
- Perform wireless networking independent security testing
- Perform Physical Security testing
- Provide PDS quality assurance, technical guidance and standards verification inspections
- Assist with development of POA&M
- Provide weekly project status reports to the ACA/SCA-V
- Develop and conduct Certification Test visit in-briefs and out-briefs, and RAWG to the System Owner (SO)

#### **AUDITING TASKS ASSOCIATED WITH CERTIFICATION OF THE INSTALLATION CAMPUS AREA NETWORK (ICAN), SYSTEMS AND APPLICATIONS**

- Review DIACAP/RMF documentation/artifact (COOP, SSP, HW/SW List, Diagrams etc.)
- Conduct certification Technical Tests (Run SCAP, ACAS, and manual STIG Reviews)
- Interview IA/IT/Cybersecurity Staff, conduct physical inspections or analyze result of inspections

- Conduct certification Technical Tests analysis and develop Test Report (ERR), Scorecard, finding Sheets and RMF Artifacts
- Review and make corrections to ACA Package Test Report (ERR), Scorecard, finding Sheets) and RMF artifacts in accordance with Risk Assessment Working Group (RAWG) comments.
- Deliver Scorecards and RMF artifacts to the TdB or SIPR Dump site or other identified data site.

#### **ADDITIONAL IA SERVICES**

It is anticipated that during the performance period IA issues may arise where the Government may request the Contractor to assist, should the Contractor staff possess the required skills to perform the requirement. All work so designated shall be temporary in nature to fill an urgent need. The Contractor shall assess impact to service level and notify the QAE. Should the QAE and Contractor not be able to reach agreement on level of impact, the disagreement shall be elevated the TBO COR and GSA COR with further elevation to the CO, if needed.

The Contractor shall perform network scanning and incident response, security engineering analysis, establish and perform test procedures, establish test environments, and execute security certification tests/demos/evaluations. The Contractor shall document results, develop reports, reach logical conclusions, and provide recommendations as well as recommending Standard Operating Procedures to alleviate the issue and/or prevent reoccurrence.

The Contractor must be capable of designing and configuring security tools, conceptualizing and implementing security systems and architectures.

The Contractor shall identify and mitigate security risks and vulnerabilities in accordance with policies, requirements, standards, practices, or procedures to correct identified vulnerability in order to sustain a government defined acceptable level of risk.

The Contractor must provide privileged user level training on IA and policies. Additionally the Contractor must provide training on Retina/ACAS, Q-TIP, eMASS, RMF and other Security Content Automation Protocol (SCAP) compliant network scanning tools in use by USAREUR at the user level.

Specific tasks may include:

- Management of the Network Policy Violation program to include coordination with Units, creation of weekly slides to brief leadership on current violations and trends.
- Process completed violation actions to the DAA for account reinstatement decision.
- Daily monitoring of Remedy and/or TMT.
- Develop SOPs and TTPs for branch processes.
- Process Request for Changes (RFC) for firewall ACL change requests. Ensure the Port, protocol and services are on the approved DISA list and coordinated with requestors.
- Process SIPR write requests (Data Transfer Authority or DTA) through Remedy.
- Provide Cyber Exercise support throughout USAREUR.

#### **SCHEDULING AND SERVICE LEVELS**

The Government will Schedule to identify C&A packages or ACA audits for Contractor action. The Government must schedule the work in a manner not to impede the Contractor's ability to meet the service level. The Government may trade off 8 C&A packages for 1 ACA Audit upon their discretion or 1 audit for 8 packages not to exceed a total of 15 audits. The contractor will acknowledge the tasking, address any concerns then assign staff accordingly.

**For the USAREUR G6 Cybersecurity (CSD) Mission:**

- Customer Support Efforts for Accreditation – the Government expects the need for 80 packages and/or RMF Self-assessments support
- ACA Audits – the Government expects the need for 9 audits

For C&A packages, the contractor shall notify the QAE within 1 business day of client related issue which will impact the agreed upon completion date. In addition, the Contractor lead will coordinate any changes to C&A artifact deliverable dates due to Government directed re-tasking on a weekly basis.

For ACA Audits, the contractor shall notify the QAE not later than the close of business the same day a client related issue occurs which will impact the agreed upon completion date.

#### **5.18 CONFIGURATION MANAGEMENT**

The Contractor shall follow USAREUR's Configuration Management Plan, processes, and procedures providing configuration management of the USAREUR C2 and C4 networks and systems. The Contractor shall provide configuration management of hardware, software, personnel, networks and documents covered by this effort. The Contractor shall participate in design reviews, maintain and report, inventory and manage Change Requests. The Contractor shall provide status and technical assistance for Configuration Control Board meetings, system fieldings and the life cycle replacement process. The Contractor shall monitor changes and create "roll back" plans. The Contractor shall provide logistics management services for the systems, equipment and materials covered under this task order, as required for the sustainment life cycle. The Contractor shall coordinate the transportation, relocation, replacement, decommissioning, shipping, staging, and receiving of equipment and materials owned by the organization, as necessary to meet mission's demands.

The Contractor shall perform configuration management support for software and system baselines according to industry best practices and USAREUR specific guidelines.

The Contractor shall:

- Provide a structured process to manage the baseline configurations and all IT assets owned by the organization.
- The Contractor shall provide configuration management of hardware, software, personnel, networks and documents covered by this effort.
- Participate in design reviews
- Change Requests (maintain and report, inventory and manage)
- Configuration Control Board (status, technical assistance, meetings, system fieldings and the life cycle replacement process)
- The Contractor shall monitor CCB changes and create "roll back" plans.
- The Contractor shall maintain and update the inventory and configuration data contained within the automated configuration management databases (CMDB).
- The Contractor shall provide procurement and logistics management services for the systems, equipment and materials covered under this task order, as required for the sustainment life cycle. The Contractor shall coordinate the procurement, transportation, relocation, replacement, decommissioning, shipping, staging, and receiving of equipment and materials owned by the organization, as necessary to meet mission's demands.

#### **5.19 REQUIREMENTS ANALYSIS SERVICES**

The Contractor shall assist the Government in assessing system performance, planning for new and evolving C4 systems, evaluating proposals for the migration of existing functionality, and making recommendations for corrections and enhancements. Contractor planning services shall include providing draft documentation and technical input to documentation for assessments, plans, system implementations and architectures, and

engineering designs related to new, evolving, and existing C4 systems. At the direction of the Government the Contractor shall conduct and/or participate in strategic planning, studies, and evaluations to provide resource requirements, present recommended solutions, determine labor and tools estimates, and plan/refine schedules. As directed by the Government, the Contractor shall perform analysis, provide recommendations, and prepare and provide planning documentation for Government approval for the transition plan of current services into the JIE environment.

The Contractor's effort shall include:

- Providing technical studies, reviewing plans, evaluating state of the technologies prior to fielding of new releases or systems
- Reviewing C4 plans and policies and providing observations and questions for consolidated responses
- Researching and coordinating technical issues and requirements and drafting new and updated policy governing technical issues
- Providing technical analyses and draft reports of C4 system tests, assessments, and architectures.
- The Contractor shall participate in meetings as required by the Government to include attending conferences; technical interchange seminars; interoperability meetings; and Government briefings related to integration, migrations, and maintenance of C2, coalition, and bi-lateral system architectures.
- Coordinating project actions and providing technical advisory services to the USAREUR G2
- Managing project plans for implementing, relocating and upgrading systems and services
- Coordinating system fieldings; overseeing changes to the system architecture
- Coordinating and planning systems exercise and training support (as needed)
- Coordinating technical support for customers
- Developing liaison with units and internal/external organizations
- Performing C4I IT services requirements analysis and feasibility studies
- Developing POIs and TTPs and manage
- Meeting new requirements to solve issues, provide operations capabilities, meet mandatory policy and tasks, and take proper actions when incidents, problems and failures occur
- Planning new and evolving C4I systems, developing and/or evaluating plans for the migration of existing functionality to new platforms and architectures, assessing performance of existing systems and making recommendations for corrections and enhancements to the CM
- Strategic planning, research/studies, and evaluations to identify resource requirements, recommended solutions, associated labor level of effort estimates, and timelines/schedules
- Research, analyze, recommendation and implementation of (once approved) new technologies, products, standards, processes, tools and techniques and providing recommendations and guidance for the design, development, implementation, integration, security and management of approved products and solutions
- Development of logical, architectural and detailed designs based on technical specifications/requirements and engineering thresholds
- Production of detailed system documentation including installation instructions, configurations, troubleshooting information and development of bill of materials (BOMs), monitoring specifications and engineering implementation/integration plan (EIP)

## **5.20 TASK MANAGEMENT TOOL SUPPORT**

The contractor shall provide Software Assurance (S/A). The contractor shall provide the government Accenture TMT product suite to include TMT/client licenses. The contractor shall provide S/A which will include versioning and upgrades, patching, hotfixes, and support for DISA-required security changes or ARCERT-required IAVA security fixes. (The contract partner is expected to fully support DoD-mandates for code-related security changes within 30 days of release.)

The contractor shall provide maintenance and sustainment support. The contractor shall provide support to mission owners (current location(s): Stuttgart and Wiesbaden, Germany) as directed. The contractor shall perform troubleshooting, system restoral, migration planning, database maintenance, customer support, and problem resolution. The contractor shall have full post-access, have a Secret clearance, read and write English fluently. The contractor shall obtain and maintain appropriate certifications as required under DoD Instruction 8570.1M.

#### **ADMINISTRATOR TRAINING**

The contractor shall deliver system administrator training to the identified mission owners on an as-needed basis which will cover TMT system configurations, network and process mapping, topologies, database management, backup and restorations, disaster recovery, client and administrator access troubleshooting and problem resolution. The contractor shall provide advanced TMT and CRM training as requested to partners in established and emergent duty locations.

#### **USER TRAINING**

The contractor shall deliver on-site user training to the mission owner as required and as a minimum one-hour block of instruction twice a month during Action Officer Training. The contractor shall ensure the training covers task creation, delegation, routing, response and closure. The contractor shall assist users in determining business processes, establish hierarchical process mappings for taskings and awards workflow, develop workflow and routing within parent organizations, and continually review TMT configuration to ensure efficient and logical results. The contractor shall assess, and develop command routing topologies to ensure the fullest investment in the CRM infrastructure and provide solutions to new and unique business requirements. The contractor shall complete upgrades as directed by the government.

#### **ACCENTURE TMT LICENSES**

The contractor will purchase Avanade TMT CORE and EDGE licenses on an annual basis to sustain vendor software license assurance support.

#### **ACCENTURE TMT ENGINEERING SERVICES**

The contractor is expected to factor in semiannual direct vendor engineering site visits to perform system upgrades.

#### **5.21 NETWORK ENGINEERING SERVICES**

The contractor shall maintain and support a constant state of readiness, security, performance and availability of command or organizational tactical and strategic networks, which include: NIPRNET / SIPRNET / JWICS/ EXERCISE-SIPRNET / DSL / WIRELESS / USBICES / CENTRIX / COALITION EXERCISE networks.

- Manage and maintain command or organizational owned/operated,
- Taclane encryption devices to include installation, configuration, keying/re-keying, and troubleshooting.
- Develop and implement storage management processes using a combination of established and approved COTS/GOTS products and best business practices. Schedule and maintain full, incremental, and differential file backups and restoration tasks.
- Develop design plans for the migration of IT assets, data and users to newly established datacenter solutions as required by the mission owner.
- Assist the mission owner in the research/development and design of replacement software/hardware and associated components. Administer, maintain, and back-up SharePoint user pages / SQL databases for all mission owner activities. This task includes the provisioning and upkeep of the mission owners SharePoint design, permissions, and possible data migration from an existing site to a new location.

- Upgrade and migrate to future releases of SharePoint and SQL databases as directed.
- Manage the infrastructure that includes both physical and virtual computing platforms and snapshot technology residing on multiple mission owner networks.
- Maintain server configurations data management, patch management, and the processes of migration to new server farm platforms as directed by the mission owner.
- Design critical network paths for high availability of data in transit while also ensuring file integrity of stationary data for all mission owned/operated datacenter environments.
- Develop and deploy required Operating Systems, updates, configurations, Access Control Lists, VLANs, Port Security and scripts for tracking, patching, and mitigation of all hardware and software vulnerabilities across all mission owner networks.
- The Contractor shall design highly available networks with failover and disaster recovery capabilities IAW mission owner COOP. The Contractor shall perform backups of network configuration files for all devices and test network failover capabilities.
- The Contractor shall provide Network documentation and configuration management. The Contractor shall provide Network Management Services to include those hardware and software standards, solutions, processes, and services which encompass:
- Maintaining and providing network connectivity by networks and systems to ensure mission critical systems and operations are available with the goal of achieving Government established monthly availability rates, not including authorized or planned service interruptions or preventive maintenance;
- Installing, configuring, and maintaining the various network management systems employed on the C4 Networks;
- Monitoring the operational status and posture of the C4 Networks;
- Supporting Fault identification and management; and Fault recovery;
- Troubleshooting and correcting all network faults to maintain the operational status in a normal, continuously operational state;
- Providing Trending and Capacity Planning services to analyze and plan for the efficient utilization and management of the networks;
- Providing recommendations on enhancing performance and correcting problems as required;
- Managing backup and restore operations/capabilities;
- Supporting service level reporting and submitting logs, statistics, or analytical data, as requested by the Government;
- Providing Configuration Management and Asset Management support, to include documenting the configuration of components of the network that are under contractor control and any changes to them;
- Planning, scheduling, and implementing maintenance actions to sustain the operational viability of the networks, to include forecasting, planning, and supporting technology refreshment /insertion projects.

## **6.0 SITE-SPECIFIC MANDATORY REQUIREMENTS**

Site specific tasks are detailed below. The contractor shall be required to provide the flexibility in staffing needed to allow for such increases and decreases in workload based upon USAREUR mission requirements.

Where deemed necessary, the contractor shall negotiate in good faith to ensure a timely resolution of any task order modifications needed to ensure effective and efficient support of the mission.

## **6.1 USAREUR CHIEF OF STAFF KNOWLEDGE MANAGEMENT**

The KM is responsible for providing collaboration and knowledge management support to the Warfighter from the HQ USAREUR staff elements to the Brigade/Brigade Combat Team organizational level in garrison, military and humanitarian contingency operations, deployments, Mission Rehearsal Exercises (MRX), and other Exercises including Joint and Coalition. The KM operations covers a wide range of collaboration tools and Mission Command Networks and Systems to include Army, Joint, NATO and Coalition command and control (C2)



systems, C4I databases and knowledge management applications. The KM maps current business and communication processes, identifies knowledge gaps and inefficiencies in knowledge sharing, formulate technical assessments and incorporating industry best business practices. This includes the generation, application, management, and exploitation of Army knowledge to foster collaboration among soldiers and units in order to share expertise and experience; facilitate leader development and intuitive decision making; and support the development of organizations and teams.

Locations:

USAG Wiesbaden, Germany: Wiesbaden (Clay Kaserne)

### Site Specific Tasks

Reference:	General Definition of Tasks Applicable to Site:
A.1	<b><u>Software Systems Integration and Inter-operability Testing:</u></b> The Contractor shall support the KM in the modernization and modification of current and legacy knowledge management collaboration systems and applications.
A.2	<b><u>System Deployment:</u></b> The Contractor shall develop and implement software application/system necessary to permit sustained KM operations in strategic (garrison), tactical (deployment) and exercise (training) environments.
A.3	<b><u>System Sustainment Training:</u></b> The Contractor shall provide application/system sustainment training to US military forces as directed by the KM mission owner. The Contractor shall develop and revise training courses.
A.4	<b><u>Configuration Management:</u></b> The Contractor shall perform configuration management support for KM with USAREUR specific guidelines and provide a structured process to manage the baseline configurations and all IT assets owned by the organization.
A.5	<b><u>System Design, Engineering, and Change Management:</u></b> The Contractor shall perform design, engineering and change management of software, system and architecture(s) to support the KM.
A.6	<b><u>Knowledge Management:</u></b> The Contractor shall provide knowledge management plans, policy, and governance. Contractor supports the Government in KM planning, developing theater policy, and governing the administration of KM for Commanders to make logical decisions. The Contractor shall provide the Government input into the technical specifications and critical knowledge areas necessary for the Government to develop broad based Knowledge Management policy that covers the entire USAREUR area of operations in garrison, mission rehearsal exercise, and deployed environments. The Contractor shall perform KM design, engineering, development, testing, deployment, training, and change management of the knowledge management software, systems, and networks.
A.7	<b><u>Technical Advisory Services:</u></b> The Contractor shall serve as a subject matter expert (SME) for KM software, systems, architectures and networks supporting the KM and shall liaison with internal and external organizations and participate in technical working groups, conferences, and knowledge sharing.
A.8	<b><u>Continuity of Operations Documentation:</u></b> The contractor shall maintain documentation to detail support for mission owner tasks (supported services, processes, configurations, access controls, systems, networks, equipment, etc...) through Standard Operating Procedures (SOP's), Architecture Views other mission owner approved format for each task.
A.9	<b><u>Task Management Tool Support Services:</u></b> The contractor shall provide Software Assurance (S/A) for the government Accenture TMT product suite to include TMT/client licenses, and product server. The contractor shall provide administrator and end user training. The contractor shall

	provide custom software engineering and development of workflow routing processes to support mission owners.
--	--

The contractor shall provide the following contract services but not limited to in section 5.0 to meet requirements:

5.1 ON SITE PRESENCE

5.2 ON-CALL SUPPORT – As required

5.3 OPERATIONS AND EXERCISE SUPPORT

5.4 SYSTEM ADMINISTRATION AND MAINTENANCE SERVICES

5.5 PORTAL TECHNOLOGIES

5.6 COLLABORATION SERVICES

5.13 SYSTEM ENGINEERING/ADMINISTRATION AND MIGRATION SERVICES

5.14 CAPABILITIES PLANNING AND REQUIREMENTS ANALYSIS SUPPORT

5.16 SOFTWARE ENGINEERING/APPLICATIONS DEVELOPMENT SERVICES

5.19 REQUIREMENTS ANALYSIS SERVICES

5.20 TASK MANAGEMENT TOOL SUPPORT

**6.2 USAREUR G2 INTELLIGENCE**

USAREUR DCS-G2, is responsible to anticipate and meet USAREUR's intelligence requirements and shape the future of intelligence support to war fighting intelligence requirements throughout the European Theater. G2 is responsible to ensure Intelligence data is highly available to provide intelligence support to land forces in the EUCOM Theater. USAREUR takes exercise operational control over intelligence units assigned or attached to USAREUR, and to provide policy guidance and oversight of liaison carried out between USAREUR and other U.S. and non-U.S. intelligence and security agencies. USAREUR has developed applications and systems to meet theater unique requirements to bridge shortcomings in fielding Army-wide systems, interoperability with Joint or Service systems or integration with multinational (e.g. NATO) or coalition commands to provide guidance on plans, policies, procedures, and organizations for collecting, producing, and dissemination intelligence, and on conducting counterintelligence activities required for the security of USAREUR forces.

USAREUR G2 provides oversight for support to ensure secure, reliable, and uninterrupted availability of the Theater Top Secret/Special Compartmented Information (TS/SCI) and Collateral Intelligence Networks, Systems, services and applications. This includes operation, maintenance and repair of TS/SCI Joint Worldwide Intelligence Communications System (JWICS) network, systems, and Video Teleconferencing (VTC) suites; software and hardware sustainment support to design, integrate, install, test, maintain, administer, operate, train and provide software and hardware configuration of Command, Control, Communications, Computers, Servers, Data Storage Devices, and Intelligence (C4I) systems supporting US Army Intelligence, 7th Staff Weather Office, Joint, Bi-lateral, Multi-lateral, Coalition, and NATO operations. In addition to standard Army-wide C4I systems. The Contractor shall provide the Government high level architectural expertise and develop architectural products and deliverables in its responsibility to manage current and future operational and exercise architectures for USAREUR intelligence organizations. Participate in and assist the customer with operational evaluations of advanced technologies. Assist in developing

standards, processes, and tools to identify and document intelligence architectural shortfalls, resource requirements associated with current and emerging intelligence systems and concepts, and to assess resources required to achieve target architectures and design. Assist USAREUR G2 in implementing I operating a Knowledge Management (KM) process to improve tools and processes for publishing, disseminating, analyzing, and managing of intelligence information.

USAREUR G2 uses specialized and diverse engineering and information technology skill sets to support the intelligence mission and multi-national Alliance partnering efforts in developing, designing, implementing, and transforming Knowledge Management processes, intelligence platforms, operational and exercise architectures. The USAREUR G2 provides direct support at but not limited to the European Foundry Site, European Intelligence Readiness Operations Center (IROC-E), Multinational Intelligence Readiness Operations Center (MN-IROC), Global Intelligence Support Activity – Europe (GISA-E) and Combined Intelligence Center (CIC).

Locations:

USAG Wiesbaden, Germany: Wiesbaden (Clay Kaserne); Darmstadt, Germany (Dagger Complex)

USAG Bavaria, Germany: Grafenwoehr, Germany (Main Post)

Site Specific Tasks

Reference:	General Definition of Tasks Applicable to Site:
B.1	<b>Configuration Management:</b> The Contractor shall perform configuration management support for G2 with USAREUR specific guidelines and provide a structured process to manage the baseline configurations and all IT assets owned by the organization. The Contractor shall maintain and update the inventory, Life Cycle replacement, and configuration data contained within the automated configuration management databases (CMDB).
B.2	<b>System Engineering Services:</b> The Contractor shall provide systems engineering and support for current and emerging Communications and Information Systems (CIS) architectures and technology platforms, Active Directory integration and Group Policy requirements, software engineering, development and integration services and, as required, CIS and technology solutions to optimize USAREUR G2 operations.
B.3	<b>Network Engineering Services:</b> Maintain and support a constant state of readiness, security, performance and availability of G2 tactical and strategic networks, which include: NIPRNET / SIPRNET / JWICS/ EXERCISE-SIPRNET / DSL / WIRELESS / USBICES / CENTRIX / BI-LATERAL / MULTI-LATERAL / COALITION / PARTNER NATION /NATO operational, deployment and exercise networks. Schedule and maintain full, incremental, and differential file backups and restoration tasks for the Intelligence Processing Center (IPC).
B.4	<b>Web Design and Application Development Services:</b> Supports in the development, implementation, operation and maintenance of commercial and highly customized web applications, built in .NET with related Microsoft SQL databases to include customizations done on Microsoft SharePoint 2007/2010 enterprise platforms. Web application support extends to all 3 networks: Unclassified (NIPR), Collateral SECRET (SIPR), and TOP SECRET/SCI.
B.5	<b>Information Systems Support:</b> The Contractor shall provide focalized technical help desk, VTC, customer support services for desktop and custom built applications and operating systems that include but are not limited to Microsoft Windows, Sun Solaris and UNIX, Administration of Windows 2008 Server OS and Active Directory.

<b>B.6</b>	<b><u>INTEL Enterprise Architect:</u></b> The contractor shall provide high level architectural products and deliverables in order to manage current and future operations and exercise architectures for USAREUR Intelligence organizations in the European Theater. Formulate transition, integration, implementation and upgrade strategy of systems and designs for intelligence infrastructure and systems in support of USAREUR missions development standards, processes and tools to identify and document intelligence architectural shortfalls, resource requirements associated with current and emerging intelligence systems and concepts and to assess resources required to achieve target design. The contractor shall develop architectures that are interoperable with NATO architectures and multi-national partners including the Multi-National Intelligence Readiness Operations Center (MN-IROC) and Exercise Architectures compliant with the Joint Exercise Life Cycle (JELC) process. Provide on-site integration and troubleshooting services.
<b>B.7</b>	<b><u>Continuity of Operations and Disaster Recovery (DR):</u></b> The contractor shall maintain the remote DR site equipment and ensure uninterrupted and verified data replication.
<b>B.8</b>	<b><u>Programs and Engineering Services:</u></b> The Contractor shall provide the Government technical support in its responsibility to manage the Transformation and other projects for the USAREUR G2.
<b>B.9</b>	<b><u>Enterprise Architecture Services:</u></b> The Contractor shall provide the Government high level architectural expertise and develop architectural products and deliverables in its responsibility to manage current and future operational and exercise architectures for USAREUR intelligence organizations. <ul style="list-style-type: none"> <li>• Participate in and assist the customer with operational evaluations of advanced technologies.</li> <li>• Assist in developing standards, processes, and tools to identify and document intelligence architectural shortfalls, resource requirements associated with current and emerging intelligence systems and concepts, and to assess resources required to achieve target architectures and design.</li> <li>• Assist USAREUR G2 in implementing I operating a Knowledge Management (KM) process to improve tools and processes for publishing, disseminating, analyzing, and managing of intelligence information.</li> <li>• Assist in developing, designing, implementing, and transforming intelligence platforms including the European Foundry Site, European Intelligence Readiness Operations Center (IROC-E), Multinational Intelligence Readiness Operations Center (MN-IROC), Global Intelligence Support Activity – Europe (GISA-E) and Combined Intelligence Center (CIC).</li> <li>• Participate in planning, designing, documenting and implementing Exercise Architectures following the Joint Exercise Life Cycle (JELC) process and provide on-site integration and troubleshooting.</li> </ul>
<b>B.10</b>	<b><u>Continuity of Operations Documentation:</u></b> The contractor shall maintain documentation to detail support for mission owner tasks (supported services, processes, configurations, access controls, systems, networks, equipment, etc...) through Standard Operating Procedures (SOP's), Architecture Views other mission owner approved format for each task.

The contractor shall provide the following contract services but not limited to in section 5.0 to meet requirements:

5.1 ON SITE PRESENCE

5.2 ON-CALL SUPPORT – As required

5.3 OPERATIONS AND EXERCISE SUPPORT

5.4 SYSTEM ADMINISTRATION AND MAINTENANCE SERVICES  
5.8 CUSTOMER SUPPORT SERVICES  
5.10 COALITION NETWORK SUPPORT SERVICES  
5.13 SYSTEM ENGINEERING/ADMINISTRATION AND MIGRATION SERVICES  
5.14 CAPABILITIES PLANNING AND REQUIREMENTS ANALYSIS SUPPORT  
5.15 SOFTWARE ENGINEERING/APPLICATIONS DEVELOPMENT SERVICES  
5.16 ENTERPRISE ENGINEERING AND ARCHITECTURE SERVICES  
5.17 INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION (C&A)  
5.18 CONFIGURATION MANAGEMENT SERVICES  
5.19 REQUIREMENTS ANALYSIS SERVICES  
5.21 NETWORK ENGINEERING SERVICES

### **6.3 USAREUR G3 MISSION COMMAND SYSTEMS DIVISION**

The G-3/3 Mission Command Support Division (MCSD) supports USAREUR classified and unclassified Mission Command Systems and programs including those on U.S., NATO and coalition networks. The major functions of MCSD are to:

- Advise the USAREUR Command Group, Staff Offices and Commanders on technical aspects of Mission Command (including engineering, planning, training, operating, securing and interfacing with higher/lower stakeholders)
- Operate and maintain U.S. and coalition theater-level Mission Command Systems including operational, exercise, cross-domain and continuity of operations plan (COOP) systems.
- Provide 24/7 operational support to Multi-National Battle Group – East (MNBG-E) Mission Command Systems
- Assume operation of the theater's Common Operational Picture ("TOP COP") in the event of a failure at EUCOM
- Provide personnel, hardware, planning and operational support to Contingency Command Post (CCP) Mission Command Systems
- Plan and support Mission Command aspects of Joint Staff, EUCOM and USAREUR led exercises

MCSD operates primarily from Wiesbaden, Germany with additional sites located at Grafenwöhr, Germany and Camp Bondsteel, Kosovo. MCSD's services are provided by direct Operation and Maintenance (O&M) of, or interfacing with, a robust set of Joint, Army, NATO and coalition nation Mission Command (MC) systems that form an agile and integrated infrastructure required to support Warfighting functions (maneuver, fires, intel, etc.). MCSD requires multiple information technology skill sets focused on this broad range of MC systems/missions.

The Contractor shall assist MCSD with this mission by planning, designing, fielding, integrating, operating, maintaining, enhancing, upgrading, sustaining and decommissioning current and future MC systems/processes. The Contractor shall assist MCSD support ongoing military operations, exercises and contingencies.

MCSD is broken into three branches: Headquarters Section, Plans Branch and Operations Support Branch. The Operations Support Branch is further sub-divided into a COP Fusion Center and a Contingency Command Post (CCP) support team. The Contractor's taskings support all of these sections.

The following list highlights the primary categories of systems operated and maintained with MCSD:

- Global Command and Control System – Joint (GCCS-J)
- Global Command and Control System – Army (GCCS-A)

- Battle Command Common Services (BCCS)
- Joint Automated Deep Operations Coordination System (JADOCS)
- Multilateral Interoperability Programme (MIP)
- Command Post of the Future (CPOF)
- Radiant Mercury (RM)
- Force XXI Battle Command, Brigade-and-Below (FBCB2) Blue Force Tracking (BFT)
- Command Web (OWF)

The G3 MCSD estimates 10-12 exercises to be supported each year.

Locations:

USAG Wiesbaden, Germany: Wiesbaden (Clay Kaserne)

USAG Bavaria, Grafenwoehr, Germany (Main Post)

Area Support Team – Balkans (Camp Bondsteel)

**Site Specific Tasks**

Reference:	General Definition of Tasks Applicable to Site:
C.1	<b><u>Management, Operations and Maintenance of Network Services:</u></b> The contractor shall support MCSD with Network Management Services to support a constant state of readiness and availability of mission owner operational and exercise networks, which may include but is not limited to: NIPRNET / SIPRNET / Wireless / CENTRIX / JWICS/ BICES/ Multinational / Coalition / Exercise. Networks can be located in garrison, deployment areas, exercise environments and/or other designated locations. The administrator shall perform the full spectrum of traditional network administration functions.
C.2	<b><u>Plans and Programs:</u></b> The contractor shall support MCSD with technical support in its responsibility to manage the Mission Command System (MCS) programs. The contractor shall provide research and recommend best practices IAW current regulations using communicated means such as Technical and White Papers. The contractor shall participate in technical forums, meetings, and working groups in order to represent MCSD's capabilities and functions; also to take away RFI's pertaining to MCSD. The contractor shall monitor and administer, and analyze taskers in order to harvest MCSD participation and requirements.
C.3	<b><u>Mission Command System Administrator:</u></b> The Contractor shall perform system administration, operation and maintenance of the USAREUR Mission Command Systems (MCS), such as but not limited to, the Global Command & Control System - Joint and Army (GCCS-J & GCCS-A), Battle Command Common Services (BCCS) stack, MS Windows Domain administration, Host Based Security System (HBSS) and cloud environments. The contractor shall provide top-level Common Operational Picture (COP) services management. The system administrator shall perform the full spectrum of traditional system administration functions such as performance, capacity, capabilities and security monitoring to ensure optimal system operation and availability is maintained; perform server backup; troubleshoot and repair or restore servers as required to resolve any issues with the system; Implement configuration changes, patches and upgrades; As required, coordinate with other agencies to



	accomplish tasks and provide system status updates. All tasks are performed within the existing infrastructure such as Solaris, Windows and Redhat OS for servers and clients on physical and virtual environment like VMware. The contractor shall build and maintain Mission Command clients. The contractor shall provide support in garrison and in a deployed austere environment as required.
<b>C.4</b>	<b><u>Mission Command System Database Administrator:</u></b> The contractor shall perform the full spectrum of traditional database (DB) administration such as performance, capacity, capabilities and security monitoring to ensure optimal system operational and availability is maintain; Perform DB backup; troubleshoot and repair or restore database as required to resolve any issues with the system; implement configuration changes, patches and upgrades; as required coordinate with other agencies to accomplish tasks; provide DB status as required. All tasks are performed on database systems, such as but not limited to, Oracle and Sybase.
<b>C.5</b>	<b><u>Strategic Mission Command Systems Program Analysis, Planning and Integration:</u></b> The contractor shall perform complex mission command and control program functions, such as architecture requirements analyses, implementation and integration plan development.
<b>C.6</b>	<b><u>Mission Command System Enterprise Architect:</u></b> The contractor shall provide Mission Command System (MCS) Enterprise Architecture (EA) subject matter expertise and recommend improvements and implementation of best business practices IAW regulatory guidance. The contractor shall provide high level C2 system architectural expertise and develop architectural products and deliverables, manage current and future COP reporting requirements. The contractor shall assist in developing standards, processes, and tools to identify and document: architectural shortfalls, resource requirements associated with current and emerging technologies to achieve an integrated C2 systems COP architecture.
<b>C.7</b>	<b><u>Mission Command Systems Engineering:</u></b> The contractor shall provide continued theater level systems engineering support for the USAREUR Mission Command System (MCS) network and Cross Domain Solutions (CDS). The contractor shall perform complex multi-disciplined analysis and prepare detailed reports/presentations on MCS projects and programs. Some of these tasks include, but are not limited to, providing experience and advice on use of networks such as SIPRNET, NIPRNET, Coalition (i.e. USBICES, SEAGULL), and exercise (i.e. JTEN, ACME) networks.
<b>C.8</b>	<b><u>Software Engineering/Web Support:</u></b> The contractor shall provide development support using server and client side technologies, including but not limited to, Ozone Widget Framework (OWF), Java, JavaScript and HTML5 to expose disparate situational awareness feeds in a geospatial manner by interfacing with various data sources such as GCCS-J, GCCS-A, etc. on Solaris, Linux and Windows Operating Systems. The contractor shall provide support in garrison and in a deployed austere environment as required.
<b>C.9</b>	<b><u>Cross-Domain Solution (CDS)/Senior Project Engineer:</u></b> The contractor shall install, configure, operate and maintain CDS systems; collect user requirements; create/edit rules-sets to meet requirements; coordinate and obtain CDS accreditation ICW CDS PM and other agencies; all tasks are performed on CDS systems, such as but not limited to, Radiant Mercury (RM) to support operations and/or exercises.

<b>C.10</b>	<b><u>Mission Command Support/Blue Force Tracker - Task Force Falcon:</u></b> The contractor shall maintain a forward deployed Field Engineering / System Administrator presence to support deployed U.S. forces in Kosovo, scheduled 6 days a week and 10 hours a day. The contractor shall operate, maintain, install, de-install, and configure Blue Force Tracking (BFT) hardware (vehicle-based and TOC kits). The contractor shall perform operations and maintenance of forward deployed USAREUR Mission Command Systems (MCS) Common Operation Picture (COP) systems.
<b>C.11</b>	<b><u>Warfighter Support:</u></b> The contractor shall support the Warfighter by providing expertise in Command and Control systems during missions that may be but not limited to: Non-Combatant Evacuation Operations (NEO), Humanitarian Assistance, Consequence Management, Disaster Relief, Peace Enforcement, and Security Cooperation / Partnership Building.
<b>C.12</b>	<b><u>Technical Advisory Services:</u></b> The Contractor shall serve as a subject matter expert (SME) for Mission Command and Control software, systems, architectures and networks supporting G3 and shall liaison with internal and external organizations and participate in technical working groups, conferences, and knowledge sharing. The contractor shall provide technical direction between USAREUR and various DoD programs.
<b>C.13</b>	<b><u>Continuity of Operations Documentation:</u></b> The contractor shall maintain documentation to detail support for mission owner tasks (supported services, processes, configurations, access controls, systems, networks, equipment, etc...) through Standard Operating Procedures (SOP's), architecture views and other mission owner approved formats for each task.
<b>C.14</b>	<b><u>Cyber Security:</u></b> The contractor shall perform computer security technical and administrative duties to include applying patches and security configurations IAW polices and regulations, coordination of systems/applications security changes and updates with systems' PM, coordination of systems security status with enterprise security managers, and manage/track patches and vulnerabilities throughout the USAREUR Mission Command Systems (MCS) network. The contractor shall employ technologies such as Windows Server Update Services and other scanning/management tools as directed by Mission Command PM.

The contractor shall provide the following contract services but not limited to in section 5.0 to meet requirements:

- 5.1 ON SITE PRESENCE
- 5.2 ON-CALL SUPPORT – As required
- 5.3 OPERATIONS AND EXERCISE SUPPORT
- 5.4 SYSTEM ADMINISTRATION AND MAINTENANCE SERVICES
- 5.5 PORTAL SERVICES (SharePoint)
- 5.12 COMMAND AND CONTROL (C2) SYSTEMS & APPLICATIONS SERVICES
- 5.13 SYSTEM ENGINEERING/ADMINISTRATION AND MIGRATION SERVICES
- 5.15 SOFTWARE ENGINEERING/APPLICATIONS DEVELOPMENT SERVICES
- 5.17 INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION (C&A)**
- 5.18 CONFIGURATION MANAGEMENT SERVICES
- 5.19 REQUIREMENTS ANALYSIS SERVICES

## 5.21 NETWORK ENGINEERING SERVICES

### 6.4 USAREUR PROVOST MARSHALL OFFICE – INSTALLATION ACCESS CONTROL SYSTEM (IACS) OPERATIONS SUPPORT

The USAREUR Office of the Provost Marshal (OPM) advises the Commanding General, and provides USAREUR policy on law enforcement, physical security, customs, biometrics, and vehicle registration operations. OPM is responsible for program management and administrative oversight for the Installation Access Control System (IACS) at all Access Control Points (ACP) within the USAREUR AOR. IACS operates on the Non-Secure Internet Protocol Router (NIPR) backbone in IPsec in transport mode. IACS is a Army program of record software with its own Authority To Operate (ATO). OPM is located on Clay Kaserne in Wiesbaden, Germany.

#### Locations:

USAG Wiesbaden, Germany; Wiesbaden (Clay Kaserne)

USAG Rheinland Pfalz, Germany: Germersheim (Germersheim Army Depot)

#### Site Specific Tasks:

Reference:	General Definition of Tasks Applicable to Site:
D.1	<b>Access Control Point Implementation Support:</b> ACP support shall include project coordination; site survey; design and engineering; equipment identification; equipment repair, and life cycle replacement. Upon Government approval the Contractor shall proceed with required procurement, surveys, assembly, installation, de-installation, movement, QA, testing, preventive maintenance and system activation.
D.2	<b>IACS Installation Component Management Support:</b> The Contractor shall proactively manage, monitor, and decommission installation asset inventories. The Contractor shall ensure critical installation components are available to fulfill IACS installation requirements and meet installation and life cycle replacement schedules.
D.3	<b>IACS Counter Terrorism and Law Enforcement Data Support:</b> The Contractor shall input, perform analysis, formulate reporting and coordinate relevant counter terrorism data from USAREUR G2, 66 <sup>th</sup> Military Intelligence Brigade, DIA, FBI, Criminal Investigation Division (CID), USAFE OSI, NAVEUR NCIS offices and other International (e.g. INTERPOL) and host nation law enforcement agencies to ensure individuals with terrorist/criminal records/histories or use of a stolen international ID are denied access using IACS.
D.4	<b>IACS Biometric/Counter Terrorism/Liaison Support:</b> The contractor shall provide programming and technical input to enable IACS to biometrically screen all IACS access requests. The contractor shall provide input to the USAREUR biometric program by conducting research and analysis to assess developments and trends on terrorism, organize crime and insider threats in coordination with various Federal, DoD, Army, EUCOM, host nation, and USARUER agencies to deny access using IACS.
D.5	<b>Continuity of Operations Documentation and Training Support:</b> The contractor shall maintain documentation to detail support for mission owner tasks (supported services, processes, configurations, access controls, systems, networks, equipment, etc...) through Standard Operating Procedures (SOP's), Architecture Views other mission owner approved format for each task and maintains them on various media sites. The contractor shall develop just-in-time training for IACS users when deficiencies are identified and new capabilities/upgrades are implemented. The contractor shall provide IACS users hands-on training throughout the theater, as required.
D.6	<b>Project / Operational Management:</b> The contractor shall provide daily IACS operations

	management oversight, to include all maintenance, engineering, upgrade implementation, Quality Assurance and life cycle support activities. The contractor shall provide technical solutions, risk assessments, equipment/manpower requirements, cost estimates, and schedule, as required. The contractor shall provide integration and coordination support as required between IMCOM-E, USAREUR, 5 <sup>th</sup> Signal, and Defense Manpower Data System (DMDC) on IACS operations.
--	---

The contractor shall provide the following contract services but not limited to in section 5.0 to meet requirements:

- 5.1 ON SITE PRESENCE
- 5.2 ON-CALL SUPPORT – As required
- 5.4 SYSTEM ADMINISTRATION AND MAINTENANCE SERVICES
- 5.8 CUSTOMER SUPPORT SERVICES
- 5.12 COMMAND AND CONTROL (C2) SYSTEMS, APPLICATIONS AND SERVICES
- 5.13 SYSTEM ENGINEERING/ADMINISTRATION AND MIGRATION SERVICES
- 5.14 CAPABILITIES PLANNING AND REQUIREMENTS ANALYSIS SUPPORT
- 5.15 SOFTWARE ENGINEERING/APPLICATIONS DEVELOPMENT SERVICES
- 5.18 CONFIGURATION MANAGEMENT SERVICES
- 5.19 REQUIREMENTS ANALYSIS SERVICES
- 5.21 NETWORK ENGINEERING SERVICES

## 6.5 USAREUR G6 HEADQUARTERS SUPPORT DIVISION

USAREUR Headquarters Support (HSD) Division is the Information Technology (IT) service provider to Headquarters, U.S. Army Europe (HQ USAREUR). HSD is comprised of over 100 military, civilian and contract personnel, managing over 300 servers both physical and virtual, providing Full Spectrum IT support for HQ USAREUR and HQ IMCOM-E, from the office to the battlefield. HSD is an Operational and planning arm of the European IT Enterprise. HSD enhances the Enterprise by providing Mission Funded Services, enhanced baseline services and supports numerous Enterprise services; e.g. Enterprise SharePoint, Enterprise Resource Forest, consolidated public website hosting, and Theater VIP support. Additionally, HSD provides coalition network and desk top support. HSD also provides support to other Theater service component commands as required. Organizations supported include HQ U.S. Air Force Europe (USAFE), EUCOM, AFRICOM, IMCOM-E, Product Manager Joint - Automatic Identification Technology (PM J-AIT), Department of the Army Inspector General (DAIG), Defense Health Information Management Systems (DHIMS), European Regional Medical Command (ERMC), and 5th Signal Command.

Locations:

USAG Wiesbaden, Germany; Wiesbaden (Clay Kaserne)

Site Specific Tasks:

Reference:	General Definition of Tasks Applicable to Site:
E.1	<b>System Engineering Services:</b> The Contractor shall provide engineering and systems support for current and emerging Communications and Information Systems (CIS) capabilities, system engineering, configuration management and as required CIS solutions in an effort to improve HQ USAREUR customer support and service, IT system performance, and overall reliability of CIS

	capabilities while supporting legacy systems to extend their life.
<b>E.2</b>	<b>SharePoint/SQL Database Services:</b> The contractor shall provide services for the USAREUR SharePoint Portals and SQL Databases with advanced technical support.
<b>E.3</b>	<b>Software Engineering/Web Support:</b> Supports in the development, implementation, operation and maintenance of legacy software applications; commercial and highly customized web applications, built in .NET with related Microsoft SQL databases and CRM technology to include customizations done on Microsoft SharePoint 2007/2010 enterprise platforms.
<b>E.4</b>	<b>Continuity of Operations Documentation:</b> The contractor shall maintain documentation to detail support for mission owner tasks (supported services, processes, configurations, access controls, systems, networks, equipment, etc...) through Standard Operating Procedures (SOP's), Architecture Views other mission owner approved format for each task.

The contractor shall provide the following contract services but not limited to in section 5.0 to meet requirements:

- 5.1 ON SITE PRESENCE
- 5.2 ON-CALL SUPPORT – As required
- 5.3 OPERATIONS AND EXERCISE SUPPORT – As required
- 5.4 SYSTEM ADMINISTRATION AND MAINTENANCE SERVICES
- 5.5 PORTAL SERVICES (SharePoint)
- 5.6 COLLABORATION SERVICES
- 5.7 WEB/MEDIA SERVICES
- 5.8 CUSTOMER SUPPORT SERVICES
- 5.10 COALITION NETWORK END USER SUPPORT
- 5.13 SYSTEM ENGINEERING/ADMINISTRATION AND MIGRATION SERVICES
- 5.14 CAPABILITIES PLANNING AND REQUIREMENTS ANALYSIS SUPPORT
- 5.15 SOFTWARE ENGINEERING/APPLICATIONS DEVELOPMENT SUPPORT
- 5.18 CONFIGURATION MANAGEMENT
- 5.19 REQUIREMENTS ANALYSIS SERVICES
- 5.20 TASK MANAGEMENT TOOL SUPPORT
- 5.21 NETWORK ENGINEERING SERVICES

## 6.6 USAREUR G6 CyberSecurity

The USAREUR G6 CyberSecurity is responsible for the cyber security program management to ensure that command networks, systems and applications are protected and accredited iaw current NSA, DoD and Army Policy or as directed and guidance received from the USAREUR's Designated Approval Authority (DAA)/Authorizing Official (AO), USAREUR's Information Assurance Manager (IAM), EOC DAA/AO. CyberSecurity is responsible to provide services and support to ensure the confidentiality, integrity and availability of USAREUR accredited C4 networks. USAREUR requires all C4 networks be protected from network attacks, unauthorized access, service interruption and unauthorized disclosure or modification of information that is processed on them. CyberSecurity is responsible for the implementation of IA strategies for all supported networks. CyberSecurity administers the command's Certification and Accreditation functions for assigned clients; performs the Agent of the Certification Authority (ACA)/Security Control Assessor-Validator (SCA-V) auditing and with other IA requirements.

Locations:

USAG Wiesbaden, Germany: Wiesbaden, Germany (Clay Kaserne)

USAG Vicenza, Italy; Vicenza (Caserna Ederle, Del Din)

Site Specific Tasks:

Reference:	General Definition of Tasks Applicable to Site:
F.1	<b>Certification and Accreditation Packages:</b> The Contractor shall provide DoD Information Assurance Certification and Accreditation Process (DIACAP) or Risk Management Framework (RMF) services i.a.w. applicable Government directives to include DODI 8510, Army regulations, and USAREUR standards.
F.2	<b>ACA Auditing Packages:</b> The contractor shall provide ACA services as directed by and in accordance with the mission owner developed/managed schedules and procedures.
F.3	<b>Additional IA Services:</b> The Contractor shall be required (as directed) to perform support for IA incidents, testing, evaluations and exercises.
F.4	<b>Continuity of Operations Documentation:</b> The contractor shall maintain documentation to detail support for mission owner tasks (supported services, processes, configurations, access controls, systems, networks, equipment, etc...) through Standard Operating Procedures (SOP's), Architecture Views other mission owner approved format for each task.

The contractor shall provide the following contract services but not limited to in section 5.0 to meet requirements:

#### 5.1 ON SITE PRESENCE

#### 5.17 INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION (C&A)

#### 6.7 USAREUR JMTC G4 BFT

The 7th Army Joint Multinational Training Command provides dynamic training, preparing forces to execute Unified Land Operations and contingencies in support of the Combatant Commands, NATO, and other national requirements. Headquartered in Grafenwoehr, Germany, the 7th Army JMTC is the U.S. Army's largest overseas training command. The combat maneuver and simulation centers, live-fire ranges, classrooms and facilities provide realistic, tailor-made training solutions to U.S., NATO and partner-nation units and leaders. As part of the simulated training, vehicles are tracked for command and control operations through the Blue Force Tracker system which relays real time data through command and control (C2) systems with geographical mapping positioning to enable decision making by the training and exercise force commanders.

The objective is to provide a fully functional, configured and operationally tested Blue Force Tracker (BFT) system equipment to meet USAREUR training requirements. Required efforts to meet this objective are fielding and maintaining BFT systems during training exercises. Fielding consists of the installation, activation, de-installation or movement of BFT system components in identified training vehicles or fixed physical locations.

Locations:

USAG Bavaria, Germany; Hohenfels (Main Post)

Site Specific Tasks:

Reference:	General Definition of Tasks Applicable to Site:
G.1	<b>BFT Component Management/Deployment/Re-Deployment:</b> The Contractor shall provide for the management of assets, preventive maintenance, installation, relocation, de-installation and



	activation of BFT in indentified training vehicles, physical locations or other identified points within the training area or designated AOR. This task provides for BFT hardware installation, configuration, de-installation, movement, upgrade, activation and testing.
<b>G.2</b>	<b>Quality Control (QC):</b> The Contractor shall develop and use a Quality Assurance and Test plan to ensure full operational capability of the system.
<b>G.3</b>	<b>Document Technical Specifications:</b> Document the design specifications in the form of architecture views. A standard set of engineering site-specific as-built drawings shall consist of the BFT components, vehicle plans depicting locations of BFT equipment; interconnect diagrams, and systems diagrams.
<b>G.4</b>	<b>Continuity of Operations Documentation:</b> The contractor shall maintain documentation to detail support for mission owner tasks (supported services, processes, configurations, access controls, systems, networks, equipment, etc...) through Standard Operating Procedures (SOP's), Architecture Views other mission owner approved format for each task.

The contractor shall provide the following contract services but not limited to in section 5.0 to meet requirements:

5.1 ON SITE PRESENCE

5.2 ON-CALL SUPPORT – As required

5.3 OPERATIONS AND EXERCISE SUPPORT – As required

5.4 SYSTEM ADMINISTRATION AND MAINTENANCE SERVICES

5.8 CUSTOMER SUPPORT SERVICES

5.14 CAPABILITIES PLANNING AND REQUIREMENTS ANALYSIS SUPPORT

5.18 CONFIGURATION MANAGEMENT

#### **6.8 JOINT MULTI-NATIONAL READINESS CENTER (JMRC) S6**

The Joint Multinational Readiness Center (JMRC) is a forward deployed environment in the EUCOM AOR, that provides world-class training to Joint, Combined, NATO, and Service Component forces and leaders in support of the Combatant Commander. JMRC trains tailored forces and headquarters for full spectrum, joint, and combined operations. It provides Current Force, Stryker Brigade Combat Teams, and Units of Action tough, realistic, Army/Joint battle-focused training. The focus is on training adaptive leaders for full spectrum operations by integrating Joint, Interagency, Multinational (JIM) players, exploiting distributive live-virtual-constructive (LVC) capabilities, and focusing on execution of simultaneous, non-contiguous operations scenarios on the Joint Operational Environment (JOE) battlefield.

JMRC trains up to a task organized Brigade Combat Team (BCT) or Units of Action (UA) with selected division/corps and Joint Force or Multinational assets. It plans and conducts mission rehearsal exercises (MRE) and mission readiness exercises (MRX) to prepare units for operational missions, and conducts live fire exercises at the Company/Team level).

The JMRC S6 estimates 10-14 exercises to be supported each year.

Locations:

USAG Bavaria, Germany; Hohenfels (Main Post)

Site Specific Tasks:

Reference:	General Definition of Tasks Applicable to Site:
H.1	<b><u>Frequency Management Services:</u></b> The contractor shall support the mission of determining and managing specific operating radio frequencies from throughout the allocated electromagnetic spectrum for U.S. Army and joint tactical training exercises to include live and simulation events, electronic countermeasures training mission; and establishing other frequency requirements for command Control and Contingency Communications (C3); and communicate\coordinate frequency allocations with National Radio Frequency Agency Germany (NARFA-DE); and assist and manage SATCOM and TACSAT for JMRC Observer Controller Teams, US, German, and Multinational Rotational Units during training at the JMRC and associated remote sites..
H.2	<b><u>Helpdesk/Customer Support - JMRC:</u></b> The contractor shall provide Tier 1 and/or Tier 2 helpdesk supporting approximately 1300 end users consisting of JMRC Operations Group and 17 JMRC subordinate units. The contractor shall provide Tier 2 customer support for related requirements of desktop and laptop Army Gold Master imaging, and deployment, , OU management, account management, desktop support, user assistance, touch maintenance, troubleshooting and problem resolution for software applications, Smart Phones, cell phones, VTC, and laptop/desktop computer systems to include the management and sustainment of all JMRC owned and operated ancillary equipment, i.e. printers, multi-function devices / digital senders.
H.3	<b><u>Helpdesk/Customer Support – MRX:</u></b> The contractor shall provide dedicated MRX helpdesk/customer support, IMO related support up to the Tier 2 level for up to 2500 users during exercises. OU management, active directory user and Microsoft exchange account management, Microsoft Virtual Desktop Imaging, Army Gold Master imaging, (and custom imaging for CONET) of up to 600 systems per rotation, desktop support, user assistance, touch maintenance, inventory asset tracking, troubleshooting and problem resolution for software applications, system access, Smart Phones, VTC and to include the management and sustainment of all JMRC owned and operated ancillary equipment, i.e. printers, multi-function devices / digital senders.
H.4	<b><u>Network Management Support - JMRC:</u></b> The Contractor shall provide Network Management Services to include switch, router, taclane, and flypack configuration and deployment hardware and software standards, solutions, processes, and services to support a constant state of readiness and availability of MISSION OWNER tactical and strategic networks, which may include: NIPRNET / SIPRNET / DSL / WIRELESS / CENTRIX / JWICS/ GCCS/ BICES/ MULTINATIONAL/COALITION/ EXERCISE and or Other C4 NETWORKS at the designated strategic (Garrison), tactical (Deployment), exercise (Training) or other designated location(s). Will configure and manage Cisco VOIP system and configure, troubleshoot, maintain call manager and associated devices. Install, configure and maintain a network and host protection systems to include NIDS, HIDS, MAC filtering, 802.1X, and sticky MAC.
H.5	<b><u>Network Management Support – MRX Network Integrator:</u></b> Prepare and provide technical detail information for network engineers to develop an interoperable configuration for their assigned network contributions covering several OSI (Open Systems Interconnection model) layers together with the Network Contributing Mission Partner (NCMP).
H.6	<b><u>System Management Support:</u></b> The Contractor shall perform operations and maintenance of JMRC systems during the sustainment life cycle support and shall conduct systems operations, , install security patches and updates during authorized service windows and perform maintenance while in garrison and during mission rehearsal exercises, contingency operations, humanitarian operations in garrison and deployed locations on networks including NIPRNET / SIPRNET / DSL / WIRELESS / CENTRIX / JWICS/ GCCS/ BICES/ MULTINATIONAL/COALITION/ EXERCISE and or Other C4 NETWORKS at the designated strategic (Garrison), tactical (Deployment), exercise (Training) or

	other designated location(s).. Install, configure, and manage HBSS, SCCM, Antivirus Software suite, ACAS on JMRC owned multinational/coalition networks.
<b>H.7</b>	<b><u>Information Assurance Support:</u></b> The contractor shall perform information assurance support and assist in the development of JMRC's Information Assurance accreditation packages (DIACAP/RMF) for NIPRNET / SIPRNET / EXERCISE-SIPRNET / DSL / WIRELESS / CENTRIX / COALITION EXERCISE / BICES systems and networks. The contractor shall track and report user IA and 8570 training requirements and compliance via ATCTS for 1300 JMRC end users and validate training for up to 2500 rotational users. Contractor shall respond 24\7 to security incidents as they occur on any JMRC strategic, tactical, exercise or production network.
<b>H.8</b>	<b><u>Operations and Maintenance Services - MRX:</u></b> The contractor shall be responsible for web development, management and administration of the CER environment to include web mail, blogs, and numerous sites that can be updated and manipulated by the OPFOR and role players during the exercise on the OPFOR/CoNET networks. The contractor shall be knowledgeable and proficient with network effects emulation system (NE2S). . The contractor shall provide multimedia services in support of the JMRC Operations Group (OPSGRP). The contractor shall participate in the MSEL Conferences of 24-32 hours per rotation. At the conclusion of the rotation, the contractor shall participate in the government conducted JMRC internal AAR(s).
<b>H.9</b>	<b><u>System Engineering Support:</u></b> The Contractor shall perform design, deployment, operations and maintenance of CONET suite of enterprise systems of JMRC systems during the sustainment life cycle support and shall conduct systems operations and maintenance while in garrison and during mission rehearsal exercises, contingency operations, humanitarian operations in garrison and deployed locations.
<b>H.10</b>	<b><u>VTC Systems Administration:</u></b> The contractor shall provide video teleconference communication (VTC) system administration, scheduling, operation and maintenance for the all of the JMRC VTC suites on the NIPR, SIPR, Tactical and Exercise networks.
<b>H.11</b>	<b><u>Telephone Control Officer:</u></b> The contractor shall perform TCO duties and responsibilities. The contractor is responsible for the programming, issuing and accountability of all Command cell phones and end user smart devices (Blackberry/iPhones). This responsibility includes performing scheduled inventories and maintaining a database of all cell /smart devices, other peripherals/associated equipment and AUPs. The contractor will be placed on orders as the TCO.
<b>H.12</b>	<b><u>Continuity of Operations Documentation:</u></b> The contractor shall maintain documentation to detail support for mission owner tasks (supported services, processes, configurations, access controls, systems, networks, equipment, etc...) through Standard Operating Procedures (SOP's), Change Control Plans (CMP), Site Specific Project Management Plans, Change Management Boards (CMB), Architecture Views and other mission owner approved format for each task. SOPs, CMP, CMBs and PMP are requirement established in the network accreditation process.
<b>H.13</b>	<b><u>Trusted Agent and Enterprise Trusted Agent (TA and ETA) PKI Token Support:</u></b> Contractor will maintain TA or ETA status for the purpose of maintaining PKI tokens on site, requesting, receiving, provisioning, and issuing tokens to users for NIPR Administrative account and for SIPR Admins and users. Contractor will utilize registered mail services on post to ship and receive tokens. Contractor will maintain database reporting token request\issue status.
<b>H.14</b>	<b><u>SharePoint Development and Administration:</u></b> Contractor will maintain SharePoint systems and services, defined in DPWS 5.5, 5.6, 5.7, 5.15, supporting multiple SharePoint instances on CONET-OPFOR, CONET-BLUFOR, NIPR-Production and NIPR-Test.

The contractor shall provide the following contract services but not limited to in section 5.0 to meet requirements:

- 5.1 ON SITE PRESENCE
- 5.2 ON-CALL SUPPORT – As required
- 5.3 OPERATIONS AND EXERCISE SUPPORT – As required
- 5.4 SYSTEM ADMINISTRATION AND MAINTENANCE SERVICES
- 5.5 PORTAL SERVICES (SharePoint)
- 5.6 COLLABORATION SERVICES
- 5.7 WEB/MEDIA SERVICES/ADMINISTRATION
- 5.8 CUSTOMER SUPPORT SERVICES
- 5.9 ACCOUNTS MANAGEMENT AND PKI TOKEN SERVICES
- 5.10 COALITION NETWORK END USER SUPPORT
- 5.11 VIRTUAL DESKTOP INFRASTRUCTURE OPERATION AND MAINTENANCE SERVICES
- 5.13 SYSTEM ENGINEERING/ADMINISTRATION AND MIGRATION SERVICES
- 5.15 SOFTWARE ENGINEERING/APPLICATIONS DEVELOPMENT SERVICES
- 5.17 INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION (C&A)**
- 5.18 CONFIGURATION MANAGEMENT
- 5.21 NETWORK ENGINEERING SERVICES

#### 6.9 EUROPEAN THEATER PKI SERVICES

The PKI mission will increase security of all DoD unclassified and classified information systems including networks (e.g., Non-secure Internet Protocol Router Network, Secret Internet Protocol Router Network, web servers, and e-mail systems). This supports the EUCOM/AFRICOM AOR or as directed for additional DoD support.

Locations:

USAG Wiesbaden, Germany: Wiesbaden (Clay Kaserne)  
USAG Stuttgart, Germany: Stuttgart (Patch/Kelly Barracks)

Site Specific Tasks:

Reference:	General Definition of Tasks Applicable to Site:
I.1	<b>Local Registration Authority and Registration Authority Support:</b> The contractor shall provide a trained and certified LRA and RA to perform duties outlined in section 5.9 (Token Management Services)
I.2	<b>Strong Understanding of IT Infrastructure:</b> The contractor shall provide personnel with relevant experience in Windows Server Active Directory (Windows OS Certification) in order to provide help desk/troubleshooting support such as middleware configuration, windows systems errors, account provisioning, and hardware installation.
I.3	<b>PKI Team Portal Support:</b> The contractor shall provide personnel with knowledge of SharePoint workflows, document libraries and permissions. The contractor shall have experience in SharePoint client side object model and SharePoint workflow engine. The contractor shall maintain and manage the PKI Team Portal. The contractor shall maintain the master page customizations, page layouts, web/app parts and develop and maintain custom workflows. In addition, the contractor shall maintain the Trusted Agent list and DD2842 document libraries.
I.4	<b>Relational Database Support:</b> The contractor shall have working knowledge of MS Access and MS SQL database design, with at least one personnel with extensive experience and relevant DBA

	certifications. The contractor shall support 4 Access databases (RA SIPR, LRA SIPR, RA NIPR, LRA NIPR), supporting all database development/design/upgrades. These functions include but are not limited to creating new tables, queries, forms, reports, and relationships.
<b>I.5</b>	<b>Continuity of Operations Documentation:</b> The contractor shall maintain documentation to detail support for mission owner tasks (supported services, processes, configurations, access controls, systems, networks, equipment, etc...) through Standard Operating Procedures (SOP's), Architecture Views other mission owner approved format for each task.

The contractor shall provide the following contract services but not limited to in section 5.0 to meet requirements:

5.1 ON SITE PRESENCE

5.2 ON-CALL SUPPORT – As required

5.8 CUSTOMER SUPPORT SERVICES

5.9 ACCOUNTS MANAGEMENT AND PKI TOKEN SERVICES

#### **6.10 UNITED STATES AFRICA COMMAND (USAFRICOM) – J1 J8**

The J1 is responsible for resource of the Command's Strategy with agile and innovative solutions. The mission essential automated solutions in use at USAFRICOM are known as FM Tools and the Resource Information Management System (RIMS). USAFRICOM J1/J8 requires rapid automation and implementation of proprietary solutions to aid in financial analysis, program assessment, mission planning, manpower status/requirements, and personnel activities. These automated solutions will integrate with those that have been previously implemented for USAFRICOM. FM Tools is a compilation of very advanced desktop tools implemented into what is known as the daily dashboard slide deck. RIMS is a Web based enterprise solution hosted by the US Southern Command. RIMS provides automated solutions that are unique to both USAFRICOM and the US Southern Command. Some RIMS capabilities are shared by each Command, but others are unique to the individual mission. In order to accomplish an enhanced level of performance and optimization of resource management, USAFRICOM now requires rapid analysis and response to accomplish an accurate data presentation specifically provided by both FM Tools and RIMS. The objective is daily visibility by each directorate into resource availability, status and performance, with the capability of projecting needs into the future for each type and element of resource. It is essential that these tools combine data from both legacy accounting systems and the recently implemented General Fund Enterprise Business System (GFEBS) to provide a single and complete picture of USAFRICOM status of funds. USAFRICOM has identified FM Tools and RIMS to be the only automated tools that provide this capability.

Location:

USAG Stuttgart, Germany: Stuttgart (Kelly Barracks)

Site Specific Tasks:

Reference:	General Definition of Tasks Applicable to Site:
<b>J.1</b>	<b>FM Tool Development, Maintenance, Integration, and Support for daily Dashboard Slide Deck:</b> The contractor shall provide onsite personnel with proven expertise in Financial Management (FM) Tools, Resource Information Management Systems (RIMS) and the rapid production of the Dashboard Slide Deck to provide mission essential decision support information to the USAFRICOM commander and staff.
<b>J.2</b>	<b>Resource Information Management System (RIMS):</b> The Contractor shall provide support to the

	<p>USAFRICOM in maintaining full operational status of RIMS and enhance existing databases or data marts including web presentation components in use at USAFRICOM J1/J8.</p> <ul style="list-style-type: none"> <li>• Setup new employees in system</li> <li>• Conduct quarterly training on RIMs</li> <li>• Perform and provide basic helpdesk functions for users</li> </ul>
J.3	<p><b><u>Personnel and Manpower Reporting and Reconciliation:</u></b> The Contractor shall provide FM Tools and/or RIMS reporting and management capabilities necessary for identification of anomalies between disparate systems, produce algorithms for keeping them in sync, and provide utilities and capabilities necessary to assist the government in successful management and automated updates of the source systems.</p> <p>Reports:</p> <ul style="list-style-type: none"> <li>• Pull data from financial systems (GFEBs, STANFINS, GCSS-Army, LMP) for daily status of funds reports by (1) fund center level, and (2) roll report up to Command level.</li> <li>• Provide access to raw accounting data archives going back to 2007/legacy system</li> <li>• Pull data (at document number level) for conducting quarterly joint review program (JRP)</li> <li>• Open Commitments</li> <li>• Current year open obligations</li> <li>• Prior year open commitments</li> <li>• Pull iDoc reports (SPS, FCM, DTS, AXOL, PowerTrack)</li> <li>• Pull status of funds to trial balance report</li> <li>• Pull accounts receivable reports</li> <li>• Update weekly Smartbooks (Comptroller, Deputy and Budget Officer)</li> <li>• Perform ad-hoc reporting as required for taskers and special assignments</li> <li>• Compile data into excel spreadsheets and PowerPoint charts for the Comptroller/Budget Officer briefings</li> </ul>
J.4	<p><b><u>Resource Management duty - as required:</u></b> The contractor shall provide support to the USAFRICOM in maintaining full operational status of RIMS and enhance existing databases or data marts including web presentation components in use at USAFRICOM J1/J8.</p>
J.5	<p><b><u>Conversion to DOD Enterprise Systems:</u></b> The contractor shall provide technical services and expertise to assist in all aspects of the migration and cutover onto these enterprise systems hosted by DoD service providers.</p>
J.6	<p><b><u>FM Tool System Operation and Maintenance:</u></b> Contractor will be required to maintain and support all FMTools and RIMS solutions built for and utilized by USAFRICOM.</p>
J.7	<p><b><u>Continuity of Operations Documentation:</u></b> The contractor shall maintain documentation to detail support for mission owner tasks (supported services, processes, configurations, access controls, systems, networks, equipment, etc...) through Standard Operating Procedures (SOP's), Architecture Views other mission owner approved format for each task.</p>

The contractor shall provide the following contract services but not limited to in section 5.0 to meet requirements:

5.1 ON SITE PRESENCE

5.2 ON-CALL SUPPORT – As required

5.13 SYSTEM ENGINEERING/ADMINISTRATION AND MIGRATION SERVICES

5.15 SOFTWARE ENGINEERING/APPLICATIONS DEVELOPMENT SERVICES

5.18 CONFIGURATION MANAGEMENT

5.19 REQUIREMENTS ANALYSIS SERVICES



## 5.21 NETWORK ENGINEERING SERVICES

### 6.11 UNITED STATES AFRICA COMMAND (USAFRICOM) CHIEF OF STAFF (CoS) – SJS (OPTIONAL)

The AFRICOM CoS SJS is responsible for providing collaboration and knowledge management support to staff elements and to service component commands in garrison, military and humanitarian contingency operations, deployments, Mission Rehearsal Exercises (MRX), and other Exercises including Joint and Coalition. The CoS SJS operations covers a wide range of collaboration tools, task management (TMT), record management and Mission Command Networks and Systems to include Joint, NATO and Coalition command and control (C2) systems, C4I databases and knowledge management applications. The CoS SJS maps current business and communication processes, identifies knowledge gaps and inefficiencies in knowledge sharing, formulate technical assessments and incorporating industry best business practices.

Location:

USAG Stuttgart, Germany: Stuttgart (Kelly Barracks)

Site Specific Tasks:

Reference:	General Definition of Tasks Applicable to Site:
K.1	<b>Electronic records management (ERM):</b> The Contractor shall provide Technical Support Service for all matters pertaining to records management and the operation of an electronic records management (ERM) application. Services include technical project management, ERM administration and training, problem identification and resolution. The Contractor shall apply sound Project Management processes and techniques for system, software, and/or hardware upgrades, enhancements, and new endeavors. Provide requirements planning support for C4 Networks and systems, including the SLAN, ULAN, and other Business Intelligence/collaboration systems.
K.2	<b>Develop Business Case(s):</b> The contractor shall translate business needs into functional and technical requirements. Develop Business Case(s) (as needed) and produce Project Charter and/or Scope Document for Government approval prior to project initiation. Produce Project Plan which at a minimum identifies actions and activities required, cost projections, scheduling to include milestones, and deliverables. Develop project turnover documentation and procedures to include system(s) acceptance plan and training for the O&M Team.
K.3	<b>Requirements Planning and Analysis:</b> The contractor shall research, analyze, plan, recommend and implement (once approved) new technologies, standards, processes, tools and techniques, and provide recommendations and guidance in the design, development, implementation and management of products and solutions.
K.4	<b>Help Desk/Customer Support:</b> The contractor shall provide Tier 2 and customer support for IMO related requirements of OU management, account management, desktop support, user assistance, touch maintenance, troubleshooting and problem resolution for software applications, Smart Phones, VTC, and laptop/desktop computer systems to include the management and sustainment of all JMRC owned and operated ancillary equipment, i.e. printers, multi-function devices / digital senders.
K.5	<b>Continuity of Operations Documentation:</b> The contractor shall maintain documentation to detail support for mission owner tasks (supported services, processes, configurations, access controls, systems, networks, equipment, etc...) through Standard Operating Procedures (SOP's), Architecture Views other mission owner approved format for each task.

The contractor shall provide the following contract services but not limited to in section 5.0 to meet requirements:

- 5.1 ON SITE PRESENCE
- 5.2 ON-CALL SUPPORT – As required
- 5.8 CUSTOMER SUPPORT SERVICES
- 5.13 SYSTEM ENGINEERING/ADMINISTRATION AND MIGRATION SERVICES
- 5.16 ENTERPRISE ENGINEERING AND ARCHITECTURE SERVICES
- 5.18 CONFIGURATION MANAGEMENT
- 5.19 REQUIREMENTS ANALYSIS SERVICES

#### 6.12 UNITED STATES AFRICA COMMAND (USAFRICOM) J2 IKD

J2 provides oversight for support to ensure secure, reliable, and uninterrupted availability of the Theater Top Secret/Special Compartmented Information (TS/SCI) Intelligence Networks, Systems, services and applications. This includes operation, maintenance and repair of TS/SCI Joint Worldwide Intelligence Communications System (JWICS) network, systems, and Video Teleconferencing (VTC) suites; software and hardware sustainment support to design, integrate, install, test, maintain, administer, operate, train and provide software and hardware configuration of Command, Control, Communications, Computers, Servers, Data Storage Devices, and Intelligence (C4I) systems supporting Joint, NATO and Coalition missions.

Location:

USAG Stuttgart, Germany: Stuttgart (Kelly Barracks)

Site Specific Tasks:

Reference:	General Definition of Tasks Applicable to Site:
L.1	<b>System Engineering Services:</b> The Contractor shall provide systems engineering, administration and support for current and emerging Communications and Information Systems (CIS) C4I Networks and systems, including but not limited to the NIPRNET / SIPRNET / EXERCISE-SIPRNET / DSL / WIRELESS / CENTRIX / BICES / COALITION / EXERCISE systems, networks architectures and technology platforms, Active Directory integration and Group Policy requirements, software engineering, development and integration services and, as required, CIS and technology solutions to optimize AFRICOM J2 operations.
L.2	<b>Requirements Planning and Analysis:</b> The contractor shall research, analyze, plan, recommend and implement (once approved) new technologies, standards, processes, tools and techniques, and provide recommendations and guidance in the design, development, implementation and management of products and solutions.
L.3	<b>Information Assurance Support:</b> The contractor shall perform information assurance support and assist in the development of JMRC's Information Assurance accreditation packages (DIACAP/RMF) for NIPRNET / SIPRNET / EXERCISE-SIPRNET / DSL / WIRELESS / CENTRIX / BICES/ COALITION / EXERCISE systems and networks.
L.4	<b>Project Management Services:</b> The Contractor shall apply sound Project Management processes and techniques for all system, software, and/or hardware upgrades, enhancements, and new endeavors.
L.5	<b>Continuity of Operations Documentation:</b> The contractor shall maintain documentation to detail support for mission owner tasks (supported services, processes, configurations, access controls, systems, networks, equipment, etc...) through Standard Operating Procedures (SOP's),

	Architecture Views other mission owner approved format for each task.
--	---

The contractor shall provide the following contract services but not limited to in section 5.0 to meet requirements:

- 5.1 ON SITE PRESENCE
- 5.2 ON-CALL SUPPORT – As required
- 5.13 SYSTEM ENGINEERING/ADMINISTRATION AND MIGRATION SERVICES
- 5.14 CAPABILITIES PLANNING AND REQUIREMENTS ANALYSIS SUPPORT
- 5.15 SOFTWARE ENGINEERING/APPLICATIONS DEVELOPMENT SERVICES
- 5.16 ENTERPRISE ENGINEERING AND ARCHITECTURE SERVICES
- 5.18 CONFIGURATION MANAGEMENT SERVICES
- 5.19 REQUIREMENTS ANALYSIS SERVICES
- 5.22 NETWORK ENGINEERING SERVICES

### 6.13 UNITED STATES EUROPEAN COMMAND (EUCOM) SECRETARY JOINT STAFF (SJS)

The EUCOM CoS SJS is responsible for providing collaboration and knowledge management support to staff elements to and service component commands in garrison, military and humanitarian contingency operations, deployments, Mission Rehearsal Exercises (MRX), and other Exercises including Joint and Coalition. The CoS SJS operations covers a wide range of collaboration tools, task management (TMT), record management and Mission Command Networks and Systems to include Joint, NATO and Coalition command and control (C2) systems, C4I databases and knowledge management applications. The CoS SJS maps current business and communication processes, identifies knowledge gaps and inefficiencies in knowledge sharing, formulate technical assessments and incorporating industry best business practices.

Location:

USAG Stuttgart, Germany: Stuttgart (Patch Barracks)

Site Specific Tasks:

Reference:	General Definition of Tasks Applicable to Site:
<b>M.1</b>	<b>Task Management Tool Support:</b> The contractor shall provide Software Assurance (S/A) for the government Avanade TMT product suite to include TMT/client licenses, and product server. Provide administrator and end user training. Provide custom software engineering and development of workflow routing processes to support mission owners.
<b>M.2</b>	<b>Continuity of Operations Documentation:</b> The contractor shall maintain documentation to detail support for mission owner tasks (supported services, processes, configurations, access controls, systems, networks, equipment, etc...) through Standard Operating Procedures (SOP's), Architecture Views other mission owner approved format for each task.

The contractor shall provide the following contract services but not limited to in section 5.0 to meet requirements:

- 5.1 ON SITE PRESENCE
- 5.2 ON-CALL SUPPORT – As required
- 5.8 CUSTOMER SUPPORT SERVICES
- 5.13 SYSTEM ENGINEERING/ADMINISTRATION AND MIGRATION SERVICES
- 5.15 SOFTWARE ENGINEERING/APPLICATIONS DEVELOPMENT SERVICES

- 5.16 ENTERPRISE ENGINEERING AND ARCHITECTURE SERVICES
- 5.18 CONFIGURATION MANAGEMENT
- 5.19 REQUIREMENTS ANALYSIS SERVICES
- 5.20 TASK MANAGEMENT TOOL SUPPORT

#### 6.14 7<sup>th</sup> MISSION SUPPORT COMMAND

7th Mission Support Command provides trained and ready, forward-stationed Consequence Management Command and Control, Civil Support Team, Civil Affairs, Enabler capabilities, as directed by USAREUR. Rapidly deploys immediate response capability and provides Title 10 responsibilities for European-based units as directed by USAREUR. Foreign Consequence Management is the assistance provided by the U.S. Government to a requesting Host Nation, with the Department of State as the Lead Federal Agency, to mitigate the effects of a deliberate or inadvertent chemical, biological, radiological, or nuclear attack or event, and to restore essential operations and services. The 7<sup>th</sup> MSC information technology uses collaboration, portal, web, information systems and network resources to enable their mission support.

Location:  
Kaiserslautern, Germany  
Grafenwoer, Germany

Site Specific Tasks:

Reference:	General Definition of Tasks Applicable to Site:
N.1	<b>Network Management Services:</b> The Contractor shall provide Network Management Services to include hardware and software standards, solutions, processes, and services to support a constant state of readiness and availability of MISSION OWNER tactical and strategic networks, which may include: NIPRNET / SIPRNET / DSL / WIRELESS / CENTRIX / JWICS/ GCCS/ BICES/ MULTINATIONAL/, COALITION/ EXERCISE and or Other C4 NETWORKS at the designated strategic (Garrison), tactical (Deployment), exercise (Training) or other designated location(s).
N.2	<b>Portal Services:</b> The Contractor shall provide the required support necessary to ensure optimal operation of the 7th MSC MOSS portal. This support includes, but is not limited to, administration, integration, and troubleshooting all aspects of the MOSS portal and associated software applications and services. The Contractor shall possess the knowledge to install additional enhancement features to the MOSS Portal (such as advanced web parts), build templates, write stored procedures, perform basic database maintenance, and deploy features.
N.3	<b>Web Management Services:</b> The Contractor shall provide Web design and Web content administrator support to maintain and improve Web-based systems. The scope of services includes planning, designing, testing, and implementing static and dynamic Web pages, Web sites, Web applications and associated content.
N.4	<b>Helpdesk/Customer Support Services:</b> The contractor shall provide Tier 2 and customer support for IMO related requirements of OU management, account management, desktop support, user assistance, touch maintenance, troubleshooting and problem resolution for software applications, Smart Phones, VTC, and laptop/desktop computer systems to include the management and sustainment of all JMRC owned and operated ancillary equipment, i.e. printers, multi-function devices / digital senders.
N.5	<b>Continuity of Operations Documentation:</b> The contractor shall maintain documentation to detail support for mission owner tasks (supported services, processes, configurations, access controls, systems, networks, equipment, etc...) through Standard Operating Procedures (SOP's),

Architecture Views other mission owner approved format for each task.
---

The contractor shall provide the following contract services but not limited to in section 5.0 to meet requirements:

5.1 ON SITE PRESENCE

5.2 ON-CALL SUPPORT – As required

5.3 OPERATIONS AND EXERCISE SUPPORT – As required

5.5 PORTAL SERVICES

5.7 WEB/MEDIA SERVICES

5.8 CUSTOMER SUPPORT SERVICES

5.13 SYSTEM ENGINEERING/ADMINISTRATION AND MIGRATION SERVICES

5.15 SOFTWARE ENGINEERING/APPLICATIONS DEVELOPMENT SERVICES

5.18 CAPABILITIES PLANNING AND REQUIREMENTS ANALYSIS SUPPORT

5.19 REQUIREMENTS ANALYSIS SERVICES

#### 6.15 409th CONTRACTING SUPPORT BRIGADE (OPTIONAL)

The 409th CSB mission is twofold. The Command serves as the Principal Assistant Responsible for Contracting (PARC) and provides the full range of contracting support throughout the USAREUR AOR. In addition, the ECC-E serves as the executive agent for contracting in Bosnia and Kosovo as designated by the EUCOM. The 409<sup>th</sup> CSB plans and executes efficient, effective and agile contracting support for USAREUR's strategic (Garrison), tactical (Deployment), exercise (Training) and contingency operations.

Information Technology is a vital enabler for the 409<sup>th</sup> CSB's mission. Contract data, internal data management, records management, official correspondence, invoicing, contract performance assessment reporting (CPAR) rely upon information technology (software applications, hardware platform) and the network infrastructure.

Location:

USAG Rheinland Pfalz, Germany: Kaiserslautern (Panzer Kaserne)

Site Specific Tasks:

Reference:	General Definition of Tasks Applicable to Site:
O.1	<b>Web Page Administration:</b> The Contractor shall provide Web design and Web content administrator support to maintain and improve Web-based systems. The scope of services includes planning, designing, testing, and implementing static and dynamic Web pages, Web sites, Web applications and associated content.
O.2	<b>Information Assurance:</b> The contractor shall perform information assurance support and assist in the development of JMRC's Information Assurance accreditation packages (DIACAP/RMF) for NIPRNET / SIPRNET / EXERCISE-SIPRNET / DSL / WIRELESS / CENTRIX / COALITION EXERCISE systems and networks.
O.3	<b>HelpDesk/Customer Support:</b> The contractor shall provide Tier 2 and customer support for IMO related requirements of OU management, account management, desktop support, user assistance, touch maintenance, troubleshooting and problem resolution for software applications, Smart Phones, VTC, and laptop/desktop computer systems to include the management and sustainment of all JMRC owned and operated ancillary equipment, i.e. printers, multi-function devices / digital senders.
O.4	<b>Knowledge Management:</b> The Contractor shall provide knowledge management plans, policy,

	and governance. Contractor supports the Government in KM planning, developing theater policy, and governing the administration of KM for Commanders to make logical decisions. The Contractor shall provide the Government input into the technical specifications and critical knowledge areas necessary for the Government to develop broad based Knowledge Management policy that covers the entire 7 <sup>th</sup> CSB AOR area of operations in garrison, mission rehearsal exercise, and deployed environments. The Contractor shall perform KM design, engineering, development, testing, deployment, training, and change management of the knowledge management software, systems, and networks.
<b>N.5</b>	<b><u>Continuity of Operations Documentation:</u></b> The contractor shall maintain documentation to detail support for mission owner tasks (supported services, processes, configurations, access controls, systems, networks, equipment, etc...) through Standard Operating Procedures (SOP's), Architecture Views other mission owner approved format for each task.

The contractor shall provide the following contract services but not limited to in section 5.0 to meet requirements:

- 5.1 ON SITE PRESENCE
- 5.2 ON-CALL SUPPORT – As required
- 5.4 SYSTEM ADMINISTRATION AND SUPPORT SERVICES
- 5.7 WEB PAGE ADMINISTRATION
- 5.8 CUSTOMER SUPPORT SERVICES
- 5.13 SYSTEM ENGINEERING/ADMINISTRATION AND MIGRATION SERVICES
- 5.16 ENTERPRISE ENGINEERING AND ARCHITECTURE SERVICES
- 5.18 CONFIGURATION MANAGEMENT
- 5.19 **REQUIREMENTS ANALYSIS SERVICES**

#### **6.16 21<sup>st</sup> THEATER SUPPORT COMMAND (OPTIONAL)**

The 21st Theater Sustainment Command sets the United States European Command (EUCOM), and as directed, the United States Africa Command (AFRICOM) theaters, employs warfighting functions in unified land operations; deploys ready forces to execute theater opening, theater distribution and sustainment; and supports the United States Army Europe (USAREUR) Theater Security Cooperation efforts to strengthen alliances and build partner capacity.

Location:  
USAG Rheinland Pfalz, Germany: Kaiserslautern

Site Specific Tasks:

<b>Reference:</b>	<b>General Definition of Tasks Applicable to Site:</b>
<b>P.1</b>	<b><u>System Management Support – Battle Command and Control:</u></b> The Contractor shall perform operations and maintenance of MISSION OWNER battle command and control systems during the sustainment life cycle support.
<b>P.2</b>	<b><u>Information Assurance:</u></b> The contractor shall perform information assurance support and assist in the development of JMRC's Information Assurance accreditation packages (DIACAP/RMF) for NIPRNET / SIPRNET / EXERCISE-SIPRNET / DSL / WIRELESS / CENTRIX / COALITION EXERCISE systems and networks.



<b>P.3</b>	<b>SharePoint Portal Support:</b> The Contractor shall provide the required support necessary to ensure optimal operation of the 7th MSC MOSS portal. This support includes, but is not limited to, administration, integration, and troubleshooting all aspects of the MOSS portal and associated software applications and services. The Contractor shall possess the knowledge to install additional enhancement features to the MOSS Portal (such as advanced web parts), build templates, write stored procedures, perform basic database maintenance, and deploy features.
<b>P.4</b>	<b>Continuity of Operations Documentation:</b> The contractor shall maintain documentation to detail support for mission owner tasks (supported services, processes, configurations, access controls, systems, networks, equipment, etc...) through Standard Operating Procedures (SOP's), Architecture Views other mission owner approved format for each task.

The contractor shall provide the following contract services but not limited to in section 5.0 to meet requirements:

5.1 ON SITE PRESENCE

5.2 ON-CALL SUPPORT – As required

5.4 SYSTEM ADMINISTRATION AND SUPPORT SERVICES

5.7 WEB PAGE ADMINISTRATION

5.8 CUSTOMER SUPPORT SERVICES

5.13 SYSTEM ENGINEERING/ADMINISTRATION AND MIGRATION SERVICES

5.16 ENTERPRISE ENGINEERING AND ARCHITECTURE SERVICES

5.18 CONFIGURATION MANAGEMENT

5.19 REQUIREMENTS ANALYSIS SERVICES

#### **6.17 IMCOM-E US ARMY GARRISON ITALY (USAG ITALY)**

The IMCOM mission is for systems accreditation and systems engineering support and to handle the day-to-day operations of the US ARMY installations in the European theater. Such day-to-day operations include Fire, Police, housing, and child-care.

The contractor shall provide systems accreditation and systems engineering support for the following systems:

1. Fire Alarm System (FAS)
2. Automated Access Control System (AACS)
3. Intrusion Detection System (IDS)
4. Direct Digital Control/Energy Management Control System (DDC/EMCS)

Location:

USAG Italy; Vicenza, Italy

Site Specific Tasks:

<b>Reference:</b>	<b>General Definition of Tasks Applicable to Site:</b>
<b>Q.1</b>	<b>Systems Accreditation Support:</b> The Contractor shall complete Interim Authority to Test (IATT) packages to be completed in order to move forward. Support will be required to execute each IATT IOT move services will require re-numbering field controllers to a new network, moving application software to VM environments, operational testing, and conformance to STIG/IAVA guidelines. Each system will start over in the accreditation process utilizing the Risk Management Framework (RMF). This will require knowledge of RMF IOT the system owner with processing

	each package through eMASS.
<b>Q.2</b>	<b>Information Assurance:</b> The contractor shall perform information assurance support and assist in the development of IMCOM's Information Assurance accreditation packages (DIACAP/RMF) for NIPRNET / SIPRNET / EXERCISE-SIPRNET / DSL / WIRELESS / CENTRIX / COALITION EXERCISE systems and networks. The contractor shall create the ATO submittal package, complete CoN submissions for software, update APMS records with appropriate system engineering cost estimates and other required data, and coordinate with DPTMS to task out data requirements to departments as required.
<b>Q.3</b>	<b>System Sizing and Scoping:</b> The Contractor establish parallel server and client systems (required to maintain operation during switchover, obtain appropriate licenses, and install/test server and client instances for each system.
<b>Q.4</b>	<b>Continuity of Operations Documentation:</b> The contractor shall maintain documentation to detail support for mission owner tasks (supported services, processes, configurations, access controls, systems, networks, equipment, etc...) through Standard Operating Procedures (SOP's), Architecture Views other mission owner approved format for each task.

The contractor shall provide the following contract services but not limited to in section 5.0 to meet requirements:

- 5.1 ON SITE PRESENCE
- 5.2 ON-CALL SUPPORT – As required
- 5.4 SYSTEM ADMINISTRATION AND SUPPORT SERVICES
- 5.8 CUSTOMER SUPPORT SERVICES
- 5.13 SYSTEM ENGINEERING/ADMINISTRATION AND MIGRATION SERVICES
- 5.16 ENTERPRISE ENGINEERING AND ARCHITECTURE SERVICES
- 5.17 INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION (C&A)

## 6.18 5<sup>th</sup> SIGNAL COMMAND (OPTIONAL)

The Mission of 5<sup>th</sup> Signal Command is to build, operate, defend, and extend network capabilities to enable mission command and create tactical, operational, and strategic flexibility for Army, Joint, and Multi-national forces in the EUCOM and AFRICOM areas of responsibility.

### 6.18.1 DWDM RS3

The Contractor shall provide dedicated onsite technical support and management of the installed DWDM OTN network. The contractor shall be familiar with the Dense Wave Division-Optical Transport Node (DWDM-OTN) network equipment. The contractor shall manage and maintain the current levels of DWDM-OTN system availability, escalating problems to the appropriate ETNOSC POC and/or vendor technical support group for assistance as necessary. The contractor shall also provide consultation and guidance to the government for troubleshooting and general system operation. The contractor shall have knowledge and experience with installing, managing/maintaining, and trouble-shooting, DWDM Optical Transport Networks. The contractor is primarily responsible for providing technical assistance to maintain current levels of System Availability. The contractor shall cover the "system administration" of the DWDM rings and optical equipment. The contractor shall assist the Transport Team in installing, managing, monitoring, administering and troubleshooting ATM/SONET/SDH and CTP networks.

The contractor shall have the expert knowledge and skills required to operate network management systems, provision and configure equipment, troubleshoot, and fault isolate system malfunctions.

The contractor shall provide the following types of on-site support services:

1. Assist in matters that relate directly or indirectly to the achievement of current levels of system performance.
2. Survey, analyze, evaluate and provide technical advice/trouble resolution pertaining to the performance and functionality of the installed system.
3. Technical assistance and training in such a manner that Government personnel will become progressively self-sufficient maintaining and operating the installed system.
4. Perform DWDM system administration and maintenance for the network. Maintain current levels of system availability utilizing the DWDM Management System.
5. Assist the principal network manager/system administrator responsible for:
  - a. Rapid detection and resolution of system failures/component failures/errors.
  - b. Network/System operation.
  - c. Routine network software and hardware installation and replacement.
  - d. Network data base backup and restore.
  - e. Audit trail and ID/password administration.
  - f. Component and system failures.
  - g. Performance of first echelon maintenance.
6. Maintain configuration management.
7. Assist in the implementation of software upgrades.
8. Emergency replacement of failed or upgraded network components. Provide on-site support if required.
9. Configuration of replaced network components.
10. Consultation and guidance to Government system operators pertaining to system generation, troubleshooting, and general system operation.
11. Assist in establishing a plan/Standard Operating Procedures (SOP) for specific O&M routines, training, qualification requirements, improved O&M method suggestion, procedures and conventions, and implementation by government personnel.
12. Assist in network engineering in support of required network re-designs due to new equipment requirements and/or equipment de-installation and removal in support of USAREUR's Global Rebasing and Restructuring (GR2) transformation.
13. Perform daily ATM/SONET/SDH/CTP administrative type functions to include but not limited to adding and deleting user accounts, creating initial setup configurations, monitoring and clearing alarms, etc.
14. The contractor shall investigate, recommend and installing enhancements and operate procedures that regulate network availability.
15. Troubleshoot networks and network applications used to manage ATM (ServiceOn Data Management), SONET/SDH (Cisco Transport Controller) and Juniper CTP (CTPView Network Management System Administration).
16. Work with network managers, 5th Signal engineers, DISA and other necessary individuals or groups to accomplish daily objectives.

#### **6.18.2 NETWORK LOAD BALANCING SUBJECT MATTER EXPERT**

Primary duties are to provide Subject Matter Expertise and configuration and operation of Cisco and Brocade load balancer hardware installed as part of CUSTOMER networks. Secondary duties are to maintain and support a constant state of readiness, security, performance and availability of networks as a member of the E-TNOSC network management team.

Load Balancer Specific Functions: The Contractor shall design highly available networks with failover and disaster recovery capabilities in accordance with COOP requirements. The Contractor shall perform backups of

network configuration files for all devices and test network failover capabilities. The Contractor shall provide Network documentation and configuration management. The specific load balancer functions for this requirement include:

- Design, configure and maintain load balancers IAW specified requirements
- Develop and implement network balancing solutions to avoid overloading risks
- Optimize server failover design to provide redundancy and COOP
- Review, evaluate, analyze, and provide recommendations for projects with devices requiring network connections to the load balancers
- Create and maintain documentation as it relates to the load balancers to include configuration management data (settings and configurations), TTPs, and O&M processes

**Network Operations Functions:** The Contractor shall perform generalized network operations as a member of a Government US Army and Dept. of the Army Civilian (DAC) and mixed contractor team. The Team provides network management services to include hardware and software standards, solutions, processes, and services. They operate, maintain, and troubleshoot the Army Enterprise routed network infrastructure and associated protocols; configure data center and campus switching and supporting protocols; and provision, operate, maintain, and troubleshoot Gigabit Ethernet, Fast Ethernet, Ethernet, and Serial circuits for the Army Enterprise Infrastructure. The Contractor, as a team member, shall provide Network Management Services to include those hardware and software standards, solutions, processes, and services which encompass:

- Maintaining and providing network connectivity to ensure mission critical systems and operations are available with the goal of achieving specified availability rates
- Installing, configuring, and maintaining specified network management systems
- Monitoring the operational status and posture;
- Supporting Fault identification/management and Fault recovery;
- Troubleshooting and correcting all network faults to maintain the operational status in a normal, continuously operational state
- Providing Trending and Capacity Planning services to analyze and plan for the efficient utilization and management of the networks
- Providing recommendations on performance enhancement and problem resolution
- Supporting service level reporting and submitting logs, statistics, or analytical data IAW specified requirements
- Providing Configuration Management and Asset Management support, to include documenting the configuration of network components and any changes made
- Planning, scheduling, and implementing maintenance actions to sustain the operational viability of the networks, to include forecasting, planning, and supporting technology refreshment /insertion projects

#### **6.18.3 DATA SCIENTIST SUPPORT**

The contractor shall provide data scientist support to work as a Splunk Architect. The contractor shall work with customer to understand the requirements and provide relevant hardware solutions to support Splunk implementation on existing networks; Development and customization of Splunk using its XML templates and advanced configuration and macros; Installation, configuration and set up of Splunk and relevant components; Users / groups creation and management; Implement security layers in the server; Breaking down the development activities and allocate to the team; Guide the team in optimal design of Splunk components and additional solution components (Python etc.); Building Splunk App, dashboards with search forms and views, packaging and distribution; Developing Scheduling alerts Experience with Deployment Server & Advanced XML;

Operational experience with a wide array of networking, relational database, security, or server virtualization technologies; Experience with Virtualization technologies (VMware ESX, MS Hyper-V).

Locations:

USAG Wiesbaden, Germany: Wiesbaden (Clay Kaserne)

Reference:	General Definition of Tasks Applicable to Site:
R.1	<b>Network Load Balancing SME Required Technical Skill Sets:</b> CCNA and/or Brocade Certified Network Engineer
R.2	<b>Data Scientist Support Required Technical Skill Sets:</b> The Contractor shall provide support with knowledge and experience in Java, C++, Python, Ruby, Perl; Experience with Regular Expressions (REGEX); Microsoft and Linux Certifications.
R.3	<b>Network Support:</b> The Contractor shall provide management and support of the Alcatel-Lucent 1695 Metropolis WSM DWDM network hardware running Alcatel-Lucent WSM ver 06.X.
R.4	<b>Continuity of Operations Documentation:</b> The contractor shall maintain documentation to detail support for mission owner tasks (supported services, processes, configurations, access controls, systems, networks, equipment, etc...) through Standard Operating Procedures (SOP's), Architecture Views other mission owner approved format for each task.

The contractor shall provide the following contract services but not limited to in section 5.0 to meet requirements:

5.1 ON SITE PRESENCE

5.2 ON-CALL SUPPORT – As required

5.8 CUSTOMER SUPPORT SERVICES

5.11 VIRTUAL DESKTOP INFRASTRUCTURE OPERATION AND MAINTENANCE SERVICES

5.13 SYSTEM ENGINEERING/ADMINISTRATION AND MIGRATION SERVICES

5.15 SOFTWARE ENGINEERING/APPLICATIONS DEVELOPMENT SERVICES

5.18 CONFIGURATION MANAGEMENT SERVICES

5.21 NETWORK MANAGEMENT SERVICES

## 6.19 IMCOM-E US ARMY GARRISON RHEINLAND PFALZ (USAG RP)

### 6.19.1 INFORMATION TECHNOLOGY SUPPORT

The contractor shall provide SharePoint developer/administrator, web developer, and Social Media administration support services for the U.S. Army Garrison Rheinland-Pfalz (USAG RP). The contractor shall be responsible for managing and providing technical expertise for the USAG RP Internet and Intranet sites including overall planning, design, architecture, availability, reliability, operations, maintenance, monitoring and security of the sites and portal. The contractor shall provide direct support and authoring of USAG RP sites, pages, databases and workflows; as well as USAG RP HTML author. The contractor shall perform routine collaboration with Project Managers and Business Process Analysts to design and develop solutions to address organizational business needs and opportunities, and propose changes to make the SharePoint, or other web-enabled environments an effective solution. The contractor shall perform analysis and design: examine requirements documents and create technical design proposals, unit and system test plans, and implementation plans for small to complex projects. The contractor shall develop concepts and decision support documentation; analyzes and implements security mechanisms to facilitate information assurance/protection and regulatory policy compliance. The contractor shall use judgment and creativity in developing, implementing and integrating systems using broad guidelines; thereby requiring interpretation and thorough familiarity with organizational

operations and mission relationships between USAG RP, IMCOM-Europe, IMCOM HQ's, and US Army Europe. The contractor shall monitor all information on the Websites and SharePoint Portal ensuring adherence to security levels and policies set by regulatory guidelines and senior leadership.

The contractor shall perform the following duties:

- Determining overall technical design and structure of Internet/Intranet sites, and evaluating new technologies
- Plan, coordinate, and accomplish studies to identify and determine the USAG RP internet administrative and technical requirements and specifications necessary to develop, modify, and implement internet sites which effectively support USAG RP
- Design, develop, and administer dynamic and static websites and SharePoint
- Creating documents for posting on the USAG RP social media sites and Intranet, including evaluation of hyperlinks, suitability and usability
- Developing the USAG RP portal pages and implementing web specific applications and interfaces
- Consulting one-on-one with Internet and Intranet customers and senior managers to evaluate user requirements and advises on design capabilities and maintenance responsibilities
- Develop local USAG RP guidelines, standard operating procedures (SOPs), bulletins and flyers concerning the operation/use of USAG RP Internet sites, services, and activities

#### **6.19.2 INFORMATION ASSURANCE ENGINEERING SUPPORT**

The contractor shall study, analyze, develop, and implement cybersecurity initiatives and policies to improve the quality, timeliness, and efficiency of cybersecurity processes. The contractor shall make recommendations and implement resolutions to a variety of conventional problems and situations related to the administration, coordination, and reporting requirements of the overall Information Systems Security Program. The work includes investigating, analyzing, and providing oral and written products/recommendations on the security and documentation system posture for GMIS systems. Failure of one of these systems to obtain necessary authorities, certification, or protection of PII can cause severe disruption of the IMCOM mission.

The contractor shall provide information assurance engineering support to the U.S. Army Garrison Rheinland-Pfalz (USAG RP). The contractor is responsible for managing and providing system security expertise for the USAG RP Garrison Mission Information Systems (GMIS) including overall planning, design, architecture, availability, reliability, operations, maintenance, monitoring and security of installation specific systems. The contractor shall work on the USAG Rheinland-Pfalz GMIS systems to bring them into Federal Information System Management Act (FISMA) compliance.

The contractor shall perform the following duties:

- Recommend, develop, test, implement, and perform:
  - a. Network and system security functions for authorized users, workstations, and servers as required under DISA and Army cybersecurity policies utilizing approved applications and procedures.
  - b. System configuration, design, and administration control procedures to enhance system performance and security for all servers, standalone systems, workstations, routers, switches, printers, scanners, Video Teleconferences (VTCs), etc.
  - c. Perform patch management and software updates for Garrison Mission Information Systems for workstation and server operating systems and applications.
  - d. Download, install, and modify IT assets in accordance with Information Assurance Vulnerabilities Assessments (IAVA) and Bulletins (IAVB).
  - e. Perform and document Contingency Planning, Annual Security Control Testing, Security reviews.



f. Configure and harden IT systems per DISA Security Technical Implementation Guides (STIGs) as required.

- Maintain current knowledge of DOD/DA/NETCOM/IMCOM security regulations and augmentation directives
- Provide assistance to system owners to ensure FISMA reporting requirements are accomplished
- Manage security testing and network assessments for Garrison system owners
- Assist the Garrison staff in answering technical and administrative problems generated from the various Directorates and Command Group
- Develop reports of analyses and processes the information in accordance with program procedures
- Provide technical input and develop documents to provide information, help prevent, and increase understanding of issues involved in computer security incidents
- Assist system owners and other representatives to create, maintain and update accreditation artifacts

Locations:

USAG Rheinland Pfalz; Kaiserslautern, Germany

Reference:	General Definition of Tasks Applicable to Site:
S.1	<b>IT Support Required Technical Skill Sets:</b> The contractor shall provide support with knowledge and experience in programming and scripting languages, Internet protocols (TCP/IP, TFP, etc.), Adobe Creative Cloud Suite, Microsoft Office, MS SharePoint, HTML software packages, system security, system management, and system backup
S.2	<b>Information Assurance Required Technical Skill Sets:</b> The Contractor shall provide support with knowledge and experience in DoD, NIST, ARMY, NETCOM Security regulations and policies; information assurance technologies/processes; change control procedures; and system/server administration.
S.3	<b>Continuity of Operations Documentation:</b> The contractor shall maintain documentation to detail support for mission owner tasks (supported services, processes, configurations, access controls, systems, networks, equipment, etc...) through Standard Operating Procedures (SOP's), Architecture Views other mission owner approved format for each task.

#### 5.1 ON SITE PRESENCE

#### 5.4 SYSTEM ADMINISTRATION AND MAINTENANCE SERVICES

#### 5.5 PORTAL SERVICES (SharePoint)

#### 5.7 WEB/MEDIA SERVICES/ADMINISTRATION

#### 5.8 CUSTOMER SUPPORT SERVICES

#### 5.11 VIRTUAL DESKTOP INFRASTRUCTURE OPERATION AND MAINTENANCE SERVICES

#### 5.13 SYSTEM ENGINEERING/ADMINISTRATION AND MIGRATION SERVICES

#### 5.15 SOFTWARE ENGINEERING/APPLICATIONS DEVELOPMENT SERVICES

#### 5.17 INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION SERVICES

### 6.VEN VENDOR SERVICES

The Contractor shall obtain (or provide the same level of service) the following vendor services on behalf of the Government to support the European theater's mission. These services shall be provided under the Tools CLIN (PWS Section 11.6.1). If the contractor proposes to provide the following vendor support services on their own, the contractor shall provide personnel with the proper certifications as highlighted in PWS Section 10.2 and in accordance with DFARS 252.239-7001. Vendor support is required as needed for services and applications that

are used by the missions listed in the PWS. The required support services may change as the technology used in theater changes.

#### **6.VEN.1 CISCO SUPPORT SERVICES**

Cisco Network Optimization Service is offered by Cisco to help customers optimize their network infrastructure to best support their mission objectives. Using Cisco expertise and best practices, Cisco Network Optimization Service helps organizations prepare their core routing and switching network to support new processes, applications, and technologies. Through assessments, strategic reviews, and ongoing network support, this service focuses on improving network performance to prepare for future changes.

Website: [http://www.cisco.com/en/US/products/ps6897/serv\\_group\\_home.html](http://www.cisco.com/en/US/products/ps6897/serv_group_home.html)

#### **6.VEN.2 EMC SUPPORT SERVICES**

EMC Residency Services comprise a range of services-from assisting with day-to-day operations and filling critical staff gaps to optimizing of processes, procedures, and support with industry best practices. EMC Residency Services deploy highly skilled, specialized professionals to address critical information management and infrastructure needs. Residency tasks may include: resource management and provisioning, monitoring of information assets, status reporting, configuration, internal or external customer support, troubleshooting, root cause analysis, documentation, and operations management.

Website: <http://www.emc.com/services/portfolio/managed-services/residency.htm>

#### **6.VEN.3 MICROSOFT IT ARCHITECTURE & PLANNING ADVISOR AND SYSTEMS MANAGEMENT TECHNICAL ASSISTANCE**

The Architecture and Planning Advisor providing access to a portfolio of strategic Microsoft technical services. Specialized IT architecture and planning services that provide visibility of improved business value of the organization's investments in Microsoft technology by obtaining assistance with your Information Technology (IT) projects in an effort to increase the effective use of Microsoft technology focused solutions. Provide reach back into Microsoft's in-depth pool of Subject Matter Experts (SME's) and Knowledge Base (KB). Provide support of Strategic Services, Architecture Alignment, Program Management and Delivery, Enterprise Infrastructure and Application Architectures, Knowledge Transfer, Solution Planning and Implementation, Operational Excellence, and Program Roadmap.

#### **6.VEN.4 NETAPP SUPPORT SERVICES**

NetApp Residency Services comprise a range of services-from assisting with day-to-day operations and filling critical staff gaps to optimizing of processes, procedures, and support with industry best practices. NetApp Residency Services deploy highly skilled, specialized professionals to address critical information management and infrastructure needs. Residency tasks may include: resource management and provisioning, monitoring of information assets, status reporting, configuration, internal or external customer support, troubleshooting, root cause analysis, documentation, and operations management.

Website: <http://www.netapp.com/us/media/ds-3175.pdf>

#### **6.OPT OPTIONAL SUPPORT SERVICES (OPTIONAL)**

##### **6.OPT.1 OPTIONAL SERVICES**

The Government reserves the unilateral right to exercise the following optional services. Options will be invoked through award of a Task Order modification issued by the Contracting Officer. Options may be invoked, in whole or in part, at the discretion of the Government. The Contractor will be provided 30-days from time of option exercise to staff positions.

At the time of exercising an option, the Government will further definitize requirements, where necessary to:

- a. Provide technical direction necessary to clearly delineate the extent of support and nature of work to be performed, deliverables and required timeframes, if any.
- b. Specify technical details about the specific environment (e.g. network, systems, applications, tools) where support is required.
- c. Identify place(s) of performance.
- d. Define the business hours in which support is required and specify requirements, if any, for providing 7-days a week, 24-hour coverage or recall during non-business hours.
- e. Identify required service level(s) and performance standards, if any.
- f. Specify security clearance requirements.
- g. Identify specific certification requirements of DoD Manual 8570.01M, Information Assurance Workforce Improvement Program applicable to the option being invoked.

#### **6.OPT.2 POTENTIAL OPTIONAL TASKS**

Options described in PWS Section 6.OPT.1 may be invoked to support USAREUR requirements of other DoD stakeholder organizations in PWS section 3.0, and/or Appendix A that falls within the scope of the requirements of this PWS.

Optional positions are anticipated to include technical skillsets similar to the labor mix performing mandatory services under this Task Order.

For proposal purposes, the Not-to-Exceed (NTE) value of this unburdened option is **\$12,400,000.00 per year**. The value of this option includes labor, ODCs, travel, and overtime support.

Examples of potential tasks and/or efforts that may impact this task order include the following but are not limited to:

#### **Regional Aligned Forces:**

As directed by the Department of the Army or the Combatant Commander, USAREUR will assume command and control of US Forces from CONUS or other home based locations as a Regional Aligned Forces (RAF). RAF will rotate on a scheduled basis within the USAREUR AOR. It is currently projected that the RAF concept will be a persistent mission for USAREUR. USAREUR will have command and control (C2) of the RAF and will integrate the RAF into the C2 operations and the JIE networks.

#### **Contingency Operations:**

As directed by the Department of the Army or the Combatant Commander, USAREUR will assume command and control of US Forces for named military and humanitarian operational and exercise missions. The operation and exercise missions are expected to be temporary and will normally have a defined start and end date. USAREUR will have command and control (C2) of the RAF and will integrate the RAF into the C2 operations and JIE networks.

#### **Surge Support:**

USAREUR mission requirements are generally well defined and supportable with existing force structure and resources. In the event that there is insufficient C4I resources to meet mission requirements, USAREUR will use contract resources for support until USAREUR internal resources are available. The Government reserves the unilateral right to exercise optional Surge support described below. The optional support will be invoked through award of a task order modification issued by the CO. Options may be invoked in whole or in part, at the discretion of the Government.

Sample Site Specific Tasks:

Reference:	General Definition of Tasks Applicable to Site:
<b>OPT.1</b>	<b><u>Frequency Management Services:</u></b> The contractor shall support the mission of determining and managing specific operating radio frequencies from throughout the allocated electromagnetic spectrum for U.S. Army and joint tactical training exercises to include live and simulation events, electronic countermeasures training mission; and establishing other frequency requirements for command Control and Contingency Communications (C3) during deployment.
<b>OPT.2</b>	<b><u>Helpdesk/Customer Support:</u></b> The contractor shall provide Tier 2 and customer support for IMO related requirements of OU management, account management, desktop support, user assistance, touch maintenance, troubleshooting and problem resolution for software applications, Smart Phones, VTC, and laptop/desktop computer systems to include the management and sustainment of all MISSION OWNED and operated ancillary equipment, i.e. printers, multi-function devices / digital senders.
<b>OPT.3</b>	<b><u>Network Support:</u></b> The Contractor shall provide Network Management Services to include hardware and software standards, solutions, processes, and services to support a constant state of readiness and availability of MISSION OWNER tactical and strategic networks, which may include: NIPRNET / SIPRNET / DSL / WIRELESS / CENTRIX / JWICS/ GCCS/ BICES/ MULTINATIONAL/COALITION/ EXERCISE and or Other C4 NETWORKS at the designated strategic (Garrison), tactical (Deployment), exercise (Training) or other designated location(s).
<b>OPT.4</b>	<b><u>System Management Support:</u></b> The Contractor shall perform operations and maintenance of MISSION OWNER systems during the sustainment life cycle support and shall conduct systems operations and maintenance while in garrison and during mission rehearsal exercises, contingency operations, humanitarian operations in garrison and deployed locations.
<b>OPT.5</b>	<b><u>Information Assurance Support:</u></b> The contractor shall perform information assurance support and assist in the development of JMRC's Information Assurance accreditation packages (DIACAP/RMF) for NIPRNET / SIPRNET / EXERCISE-SIPRNET / DSL / WIRELESS / CENTRIX / COALITION EXERCISE systems and networks.
<b>OPT.6</b>	<b><u>Continuity of Operations Documentation:</u></b> The contractor shall maintain documentation to detail support for mission owner tasks (supported services, processes, configurations, access controls, systems, networks, equipment, etc...) through Standard Operating Procedures (SOP's), Architecture Views other mission owner approved format for each task.

The contractor shall provide the following contract services but not limited to in section 5.0 to meet requirements:

5.1-5.21 ALL SERVICES

## 7.0 REPORTING REQUIREMENTS

### 7.1 WEEKLY ACTIVITY REPORTS (WAR)

The Contractor shall submit Weekly Activity Report (WAR) & or Significant Activity (SIGACT) Reports at the site level, as required on the first workday of each week. At a minimum, the report shall:

- Summarize work accomplishments during the period by task, including but not limited to: on-going activities, new activities, activities completed; progress;
- Identify planned work activities by task for the next period;
- Show staffing changes and personnel status/resource availability information, such as but not limited to: upcoming leave/vacations; incoming/outgoing personnel; completed and planned TDYs, vacancies.

## **7.2 MONTHLY STATUS REPORT**

The Contractor shall submit Monthly Status Reports (MSR) by the 15th of each month. Content of the reports should be organized by site and shall include, as a minimum, the items cited in the MTSR & MFSR below. The reports shall be posted to GSA's ITSS System and be emailed to both the USAREUR COR and the GSA COR. Where directed, the contractor shall provide site specific monthly status information to the designated Government QAEs.

Monthly Technical Summary Report (MTSR), as a minimum, shall include:

- a. Staffing matrix showing current staffing level, personnel gains, losses, vacancies, and status (security clearance; TESA; 8570/computing environment/industry certifications).
- b. Work Activities: during reporting period, by task (Include: On-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
- c. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
- d. Government actions required.
- e. Schedule (Showing major tasks, milestones, deliverables, and progress information; planned/actual start and completion dates for each project).
- f. Summary of Ad-hoc Technical Reports submitted to the Government during the reporting period.

Monthly Financial Summary Report (MFSR), as a minimum, shall include:

- a. Accumulated invoice cost for each CLIN up to the previous month.
- b. Projected cost of each CLIN for the current month and forecasts through the end of the current performance period.
- c. Summary of all Travel by Contractor personnel during the month (trips taken, conferences attended, etc.). The summary shall include, at a minimum: a description of the travel conducted, statement as to purpose, the number of persons in the party, traveler name(s), destination(s), duration of stay, and estimated/actual costs. Trip reports, (where identified as a requirement when travel is approved), shall be attached to the MSR.
- d. A projection of all Travel requirements for the upcoming month including a description of the travel planned, including a statement as to purpose, the number of persons in the party, traveler name(s), destination(s), duration of stay, and estimated cost.
- e. Summary of all Purchases during the reporting period. The summary shall include at a minimum: description, quantity, status (received, in transit, back-ordered, etc.)
- f. A projection of all anticipated staffing related ODC expenses for the upcoming month including an itemized description including a statement as to purpose, the number of persons in the party, traveler name(s), destination(s), duration of stay, and estimated cost.

## **7.3 PROGRAM METRICS**

The Contractor shall develop, at the written request of the requiring activity, a system of reporting program metrics at the site and aggregate level, for the review and approval of the Government. The metrics shall:

- a. Serve as a measure of Contractor effectiveness in meeting standards required for critical systems and VIP support.
- b. Serve as a measure of Contractor effectiveness in meeting USAREUR design and engineering project requirements.

On approval, the Contractor shall implement the metrics and provide the Government with a written monthly metrics report (segregated by site & aggregated at the Task Order level, where applicable) which:

- Provides quantitative measurements which capture and evaluate communications and information technology support, identify trends, and measure performance.
- Provides comparative monthly performance data.

Program Metrics shall be submitted concurrently with the MTSR described in 7.2. Where requested, the Contractor shall provide the Government the raw data and statistical calculations used to produce the program metrics as well as real-time access to metrics on communications and information technology support, such as actual statistics, trend analysis and performance measurements and assessments.

#### **7.4 CONTRACT ACTIVITY AND STATUS MEETINGS**

The Contractor shall convene a monthly Contract Activity and Status Meeting with the COR, QAE, and other key government stakeholders. The Contractor shall conduct the Contract Activity and Status Meeting by the fourth Thursday of each month. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activity and status report, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The Contractor PM shall provide minutes of these meetings to the COR/QAE within five calendar days following the meeting. The minutes will include list of attendees, issues discussed, decisions made, and action items assigned.

#### **7.5 QUARTERLY PROGRAM MANAGEMENT REVIEWS**

The Contractor shall administer and convene a quarterly Program Management Review (PMR) as coordinated with the COR to include key Program Stakeholders as participation is required or determined by scope of the PMR. The purpose of the PMR is to discuss key Program activities, facilitate stakeholder discussion and to provide information that supports Contract decision-making and the financial management process. Additional topics as determined by the COR may include: indepth program financials, process discussions, updates on key projects and milestones, or any other focus areas relevant to that particular audience. The scope of the PMRs will vary depending on the schedule, funding cycle and key milestones to be discussed.

The Contractor PM shall provide minutes of these meetings to the COR / QAE within five calendar days following the meeting. The minutes will include list of attendees, issues discussed, decisions made, and action items assigned.

#### **7.6 TRIP REPORTS/CONFERENCE REPORTS**

The Government will identify the need for a Trip Report (if required) or Conference Report when the request for travel is submitted to and approved by the COR. The Contractor shall keep a summary of all long-distance travel, to include, at a minimum, the name of the employee, location of travel, duration of trip, purpose, activities and outcomes, and POC at travel location.



## **7.7 CONTRACT MANAGEMENT PORTAL**

The Government will identify a Contract Management Portal in which the Contractor shall utilize during the life of this Task Order to request and/or retain Government approval to purchase Incidentals and authorize Contractor travel in support of TDYs (i.e. Tools and non-Travel ODCs).

## **7.8 PROJECT ENGINEERING PLAN**

When required, the Contractor shall provide a Project Engineering Plan (PEP) for managing the backlog of project requests. The PEP shall include schedule and status information for short term and long term projects.

## **7.9 CONTRACT MANPOWER REPORTING**

The Office of the Assistant Secretary of the Army (Manpower and Reserve Affairs) operates and maintains a secure Army data collection site where the Contractor shall report ALL Contractor manpower (including subContractor manpower) required for performance of this contract. The Contractor is required to completely fill in all the information in the format using the following website:

<https://Contractormanpower.army.pentagon.mil>. The required information includes:

- (1) Contracting Office, Contracting Officer, Contracting Officer's Technical Representative;
- (2) Contract number, including task and delivery order number;
- (3) Beginning and ending dates covered by reporting period;
- (4) Contractor name, address, phone number, e-mail address, identity of Contractor employee entering data;
- (5) Estimated direct labor hours (including sub-Contractors);
- (6) Estimated direct labor dollars paid this reporting period (including sub-Contractors);
- (7) Total payments (including sub-Contractors);
- (8) Predominant Federal Service Code (FSC) reflecting services provided by Contractor (and separate predominant FSC for each sub-Contractor if different);
- (9) Estimated data collection cost;
- (10) Organizational title associated with the Unit Identification Code (UIC) for the Army Requiring Activity (the Army Requiring Activity is responsible for providing the Contractor with its UIC for the purposes of reporting this information);
- (11) Locations where Contractor and sub-Contractors perform the work (specified by zip code in the United States and nearest city, country, when in an overseas location, using standardized nomenclature provided on website);
- (12) Presence of deployment or contingency contract language; and
- (13) Number of Contractor and sub-Contractor employees deployed in theater this reporting period (by country). As part of its submission, the Contractor shall also provide the estimated total cost (if any) incurred to comply with this reporting requirement.

Reporting period will be the period of performance not to exceed 12 months ending 30 September of each government fiscal year and must be reported by 31 October of each calendar year.

## **7.10 ADDITIONAL REPORTS OR DOCUMENTATION ASSISTANCE**

The following reports are to be develop by the Contractor, reviewed and approved by the COR/QAE prior to implementation:

The Contractor may periodically be tasked with providing input to or assisting in creation of, update, and maintenance of documentation listed below for those sections of the documents that are germane to the services provided under the scope of this T.O. Where required, the Contractor shall create, update, and/or maintain:

- Standard Operating Procedures (SOP)s
- Smart Books
- Operation Security (OPSEC) Plans
- Security Plans

All records, information and analysis developed by the Contractor in support of this contract are to be the sole property of the Government. These items may include, but are not limited to reports, meeting minutes, briefing materials, slides shows, operational needs statements, e-mails, AUTODIN and DMS messages, and data stored in any way on Government computers such as Microsoft Excel, Access, Word, PowerPoint, Share Point, Project, Visio and Outlook files.

## 8.0 TASK ORDER DELIVERABLES/SUPPLIES

The Contractor shall provide electronic copies of each deliverable. Unless otherwise specified, electronic copies shall be delivered via email attachment. The format of specific deliverables shall be proposed by the Contractor and agreed to by the Government.

Deliverables Schedule: The table below summarizes deliverables and reports that the Contractor is expected to produce throughout the performance of work described in this PWS.

## 8.1 DELIVERABLES

The contractor is expected to develop and maintain a Program Management Plan (PMP) for the supported task(s) of the mission owner. The following schedule of milestones and deliverable submission dates will be used by the Mission Owner Quality Assurance Evaluator and USAREUR COR to monitor timely progress under this Task Order.

The following abbreviations are used in this schedule:

- N/A: Not Applicable
- i.a.w.: In accordance with
- NLT: No later than
- TOA: Task Order Award
- All references to days imply workdays, unless otherwise noted

DELIVERABLES	DUE DATE / PLANNED COMPLETION DATE
Network Documentation	i.a.w. PMP
Maintenance Management Plan	i.a.w. PMP
Supported Equipment List	i.a.w. PMP
Maintenance Actions Summary Report	i.a.w. PMP
On-Call Rosters	i.a.w. PMP
Access Control Lists	i.a.w. PMP
Backup and Recovery Plan	i.a.w. PMP
COOP Exercise Reports	Annual
COOP Exercise Plan	30 calendar days prior to the anticipated start date of the exercise
Certification and Accreditation Documentation	i.a.w. PMP

DELIVERABLES	DUE DATE / PLANNED COMPLETION DATE
Security Event Logs	i.a.w. PMP
Information Assurance SOP/TTPs	i.a.w. PMP
IA Compliancy Reports	i.a.w. PMP
Plan of Action and Milestones (POA&M)	i.a.w. PMP
Engineering Assessments	i.a.w. PMP
System Documentation	i.a.w. PMP
Preliminary Studies	i.a.w. PMP
Strategic Planning Studies	i.a.w. PMP
Estimates and Schedules	i.a.w. PMP
Technical Studies	i.a.w. PMP
Draft Technical Policy	i.a.w. PMP
Network Architecture Plan	i.a.w. PMP
C4 Network Systems Documentation	i.a.w. PMP
C4 Systems Architecture Documentation <ul style="list-style-type: none"> <li>• Draft C4 Systems Architecture Technical Product</li> <li>• Final C4 Systems Architecture Technical Product</li> </ul>	i.a.w. PMP, Quarterly Updates Final Due 10 workdays after Government comment
C4 System Tests, Assessments, and Architecture Reports	i.a.w. PMP
Technical Implementation Instructions	i.a.w. PMP
Migration/Transition Planning Documentation	i.a.w. PMP
<ul style="list-style-type: none"> <li>• SME Support Activity Report</li> <li>• Audit report</li> </ul>	i.a.w. PMP
Network Configuration Documentation	i.a.w. PMP
Communications & IT Refresh/Integration Milestone Plan	Quarterly Updates
Program Management Plan (PMP, inclusive of: <ul style="list-style-type: none"> <li>• Quality Control Plan</li> <li>• Quality Assurance Plan</li> <li>• Risk Management Plan</li> <li>• Communications and Change Management processes</li> </ul>	Draft within 10 calendar days following the Kickoff Meeting  Final within 10 workdays after Government comment;  Updates, as required during performance
PMP Briefs	On 24 hours notice
Project Engineering Plan	Monthly
Contract Activity and Status Meetings Minutes	Within 5 calendar days following the monthly meeting
Monthly Status Report (MSR)	By the 15 <sup>th</sup> of each month

DELIVERABLES	DUE DATE / PLANNED COMPLETION DATE
Metrics Report	Monthly to coincide with submission of Monthly Status Report
Trip Reports	i.a.w. PMP
Technical Expert Status Accreditation (TESA) Documentation	i.a.w. PMP
Security Plan	i.a.w. PMP
After Action Reports (AAR)	i.a.w. PMP
Contractor Manpower Report	By October 31 of each calendar year
GFP and GFE Reports	NLT 30 days prior to new Option Period or TO completion
Kick-Off Meeting	Upon Task Order Award, as scheduled by the CO, COR or designated representative
Transition-In Plan	NLT 15 days following award of the Task Order
Transition-Out Plan	NLT 180 days prior to end of final performance period, or as otherwise directed by the COR
*Site Specific Deliverables will be identified on an as needed basis.	*As needed

## 8.2 DELIVERABLES MEDIA

Identified below is the range of electronic deliverable types. The Contractor shall submit electronic deliverables in a format compatible with current versions of the specified software in use by the client.

- Text – Microsoft Word
- Spreadsheets – Microsoft Excel
- Briefings – Microsoft PowerPoint
- Drawings – Microsoft Visio
- Schedules – Microsoft Project

Other file formats (example: .pdf) may be acceptable as mutually agreed and coordinated with the USAREUR COR and GSA COR.

## 8.3 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the Task Order, the Contractor's proposal and other terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with applicable clauses.

Deliverables will be inspected for content, completeness, accuracy and conformance to Task Order requirements. Inspection may include validation of information or software through the use of automated tools, testing or inspections of the deliverables.

#### **8.4 GENERAL ACCEPTANCE CRITERIA**

Deliverables will be accepted when all discrepancies, errors or other deficiencies identified in writing by the Government have been corrected. The general quality measures, set forth below, will be applied to each deliverable received from the Contractor under this task order:

- Accuracy – Deliverables shall be accurate in presentation, technical content, and adherence to accepted elements of style.
- Clarity – Deliverables shall be clear and concise; engineering terms shall be used, as appropriate. All diagrams shall be easy to understand, legible, and relevant to the supporting narrative. All acronyms shall be clearly and fully specified upon first use.
- Specifications Validity – All Deliverables must satisfy the requirements of the Government as specified herein.
- File Editing – All text and diagrammatic files shall be editable by the Government.
- Format – Deliverables shall follow Army guidance. Where none exists, the Contractor shall coordinate approval of format with the COR.
- Timeliness – Deliverables shall be submitted on or before the due date specified.

For software development, the final acceptance of the software program will occur when all discrepancies, errors or other deficiencies identified in writing by the Government have been resolved, either through documentation updates, program correction or other mutually agreeable methods.

#### **8.5 DRAFT DELIVERABLES**

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version. All of the Government's comments to deliverables must either be incorporated in the succeeding version of the deliverable or the Contractor must demonstrate to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling/grammatical errors, improper format, or otherwise does not conform to the requirements stated within this Task Order, the document may be immediately rejected without further review and returned to the Contractor for correction and resubmission. If the Contractor requires additional Government guidance to produce an acceptable draft, the Contractor shall arrange a meeting with the COR.

#### **8.6 WRITTEN ACCEPTANCE/REJECTION OF DELIVERABLES BY THE GOVERNMENT**

The Government will provide written acceptance, comments and/or change requests, if any, within fifteen (15) work days from Government receipt of the draft deliverable.

Upon receipt of the Government comments, the Contractor shall have ten (10) work days to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

The Government shall provide written notification of acceptance or rejection of all final deliverables within fifteen (15) work days. All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

## **8.7 NON-CONFORMING PRODUCTS OR SERVICES**

Non-conforming products or services will be rejected. Deficiencies will be corrected, by the Contractor, within ten (10) work days of the rejection notice. If the deficiencies cannot be corrected within ten (10) work days, the Contractor shall immediately notify the COR of the reason for the delay and provide a proposed corrective action plan within ten (10) work days.

## **9 SECURITY REQUIREMENTS**

The Government will furnish a DD Form 254 Contract Security Classification Specification at time of award (The FINAL DD254 is contained in Appendix F. The Contractor shall have a TOP SECRET Facility Clearance with NO Safeguarding requirement. The Contractor shall require access to COMSEC information, Sensitive Compartmented Information (SCI), Non-SCI information, NATO information and For Official Use Only (FOUO) information. The Contractor shall require access to the SIPRNET, JWICS and other classified systems as identified on the DD 254. The Contractor shall have access to classified at Government facilities only (OCONUS). The Contractor shall have OPSEC requirements.

### **9.1 SECURITY PLAN**

The Contractor shall develop a written plan for physical security, document and material security, and personnel security IAW DoD, U.S. Army, USAREUR and local physical security regulations. The Government will review and approve this plan, and any subsequent changes to it. The Physical Security Plan shall include all GFP provided under this task order, and shall include: Receiving, storing, disseminating, transporting, and protecting items involved in the performance of this task order and classified by the Government as Confidential, Secret, Top Secret, or Sensitive Compartmented Information (SCI). This data or information will be processed IAW DoD 5220.22-R (Industrial Security Regulation (ISR)) and DoD 5200-22-M (National Industrial Security Program Operating Manual (NISPOM)).

### **9.2 PERSONNEL SECURITY CLEARANCE**

DOD 5200.2-R, the Department of Defense (DOD) Personnel Security Program, requires active duty military, DOD civilian, DOD consultants, and support contractor personnel performing work on sensitive automated information systems (AISs) to be assigned to positions which are designated at one of 3 sensitivity levels. The levels are: IT – I, IT – II, or IT – III. These designations equate to Critical Sensitive and Non-Critical Sensitive positions. The employing contractor will ensure individuals assigned to these sensitive positions have completed the appropriate access request forms. IT Level – I – Individuals assigned to positions where damage to DOD networks and development systems can be accomplished and no checks are in place to determine potential destruction of sensitive information. The investigation requirement for these positions is completion of a Special Security Background Investigation (SSBI) with favorable results within the last 5 years. IT Level – II and III – Individuals assigned to positions where daily unsupervised access to DOD networks and information systems containing Sensitive but Unclassified or Sensitive Classified up to and including Collateral Secret information is a portion of their duties. The investigation requirement for these positions is completion of a Defense National Agency Check with Written Inquiries (NACI) with favorable results. For positions identified as IT – II and III, foreign nationals may be appointed if they: Possess a unique or unusual skill or expertise that is urgently needed for a specific DOD requirement and for which a suitable United States citizen is not available, and approved in writing by the cognizant DoD Commander. However, under no circumstances can these individuals be assigned before completion and favorable adjudication of the appropriate security investigation. In all cases, the contractor will forward employee investigation information to the designated Government Representative before assignment of these individuals on the task order and will ensure a visit request with that investigation information is provided yearly. The COR retains the right to request removal of contractor personnel, regardless of prior clearance or adjudication status, whose actions while assigned to this task order conflict with the



interests of the Government. The reason for removal will be fully documented in writing by the COR, and such documentation will be submitted to the Contracting Officer, when directed. All contractor personnel are required, prior to being granted access to networks and/or systems, to obtain the proper security clearances or Employment Authorization, read and sign the User Agreement, and attend a Security Briefing prior to being granted access to networks and/or systems.

**All contractors shall possess at least a SECRET level security clearance and Single Scope Background Investigation (SSBI) within the last 5 years to begin performance or remain working on this contract.**

The table below identifies security clearance requirements by SOW task area where the clearance level is higher than SECRET:

PWS REF.	TASK AREA/FUNCTION	TARGET SECURITY CLEARANCE LEVEL
----------	--------------------	---------------------------------

<b>4.0</b>	<b>PMO</b>	TS/SCI
<b>6.1</b>	<b>CHIEF OF STAFF KM</b>	SECRET/SSBI
<b>6.2</b>	<b>USAREUR G2</b>	TS/SCI
<b>6.3</b>	<b>HQ G3 MCSD</b>	Minimum SECRET/SSBI with ability to obtain TS/SCI as required
<b>6.4</b>	<b>PROVOST MARSHAL OFFICE, IACS</b>	50% SECRET/SSBI - 50% TS/SCI
<b>6.5</b>	<b>USAREUR G6 HSD</b>	50% SECRET/SSBI - 50% TS/SCI
<b>6.6</b>	<b>USAREUR G6 CyberSecurity</b>	SECRET/SSBI
<b>6.7</b>	<b>Joint Multinational Training Command G4</b>	SECRET/SSBI
<b>6.8</b>	<b>Joint Multination Readiness Command S6</b>	SECRET/SSBI
<b>6.9</b>	<b>European Theater PKI Services</b>	SECRET/SSBI
<b>6.10</b>	<b>AFRICOM J1 J8</b>	SECRET/SSBI
<b>6.11</b>	<b>AFRICOM CoS</b>	SECRET/SSBI
<b>6.12</b>	<b>AFRICOM J2</b>	TS/SCI
<b>6.13</b>	<b>7th Mission Support Command</b>	SECRET/SSBI
<b>6.14</b>	<b>409th Contracting Support Brigade</b>	SECRET/SSBI
<b>6.15</b>	<b>EUCOM SGS TMT</b>	SECRET/SSBI
<b>6.16</b>	<b>21st TSC</b>	SECRET/SSBI
<b>6.17</b>	<b>IMCOM-E USAG Italy</b>	SECRET/SSBI
<b>6.18</b>	<b>5SC</b>	TS/SCI
<b>6.19</b>	<b>IMCOM-E USAG Rheinland Pfalz</b>	SECRET/SSBI
<b>6.VEN</b>	<b>Vendor Services</b>	
	Cisco Support Services	SECRET/SSBI
	EMC Support Services	SECRET/SSBI
	Microsoft IT Architecture & Planning Advisor and Systems Management Technical Assistance	SECRET/SSBI
	NetApp Support Services	SECRET/SSBI
<b>6.OPT</b>	<b>OPTIONAL SUPPORT SERVICES</b>	SECRET/SSBI

### 9.3 OPERATIONS SECURITY (OPSEC)

AR 530-1 provides guidance on OPSEC. The Contractor shall familiarize all new employees and conduct refresher sessions as needed in the areas covered under this task order as part of the OPSEC Plan. Para 6-2 g of AR 530-1 lists information the Contractor shall need to implement an OPSEC plan. This information will be provided to the Contractor after award of the Task Order.

## 10 PERSONNEL REQUIREMENTS

The Contractor is expected to minimize employee turnover with respect to personnel performing on this effort; although the government recognizes that the contractor cannot compel any individual to remain under its employ. Replacement personnel proposed must be at least as qualified as the individual being replaced.

### 10.1 KEY PERSONNEL

Key personnel are considered mission critical and must be assigned for the duration of the Task Order. The Contractor shall not remove or replace any key personnel under this TO without the written concurrence of the CO, subject to the following substitution of Contractor Key Personnel procedures: The Contractor shall notify the GSACO and COR no later than ten (10) workdays in advance of any proposed key personnel substitution. Within the notice, the Contractor shall include a resume for the proposed replacement and justification in sufficient detail to permit evaluation of the impact of the change on TO performance.

Substitute personnel qualifications shall be equal to or greater than those of the person being substituted. If the CO and the COR determine that the proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the substitution will be denied and the Contractor shall propose an alternate candidate. If any designated key personnel are subcontractor personnel, the Contractor shall include the substance of this clause in any subcontract that is awarded under this TO.

Requirements for Govt. Specified Key Personnel			
TASK AREA/FUNCTION	8570 Requirements	Required CE Certification / Industry Credential	Experience Requirement
PROGRAM MANAGEMENT			
Program Manager	IAT II	PMP and/or ITIL Expert	Experience managing a program or task order of this size and magnitude.
USAREUR G2			
Enterprise Architecture Services	IAT II	PMP, MCITP or other associated industry certification	Must have experience providing the Government high level architectural expertise and developing DODAF or industry equivalent architectural products.
USAREUR G3 MCSD			
MCSD Plans & Programs	IAT II	CISSP and/or CAPM	Experience providing theater level Mission Command (MC)/Command and Control (C2) systems engineering support

			Command network and Cross Domain Solution (CDS) Trusted Guard/Radiant Mercury systems.
<b>MCSD Plans &amp; Programs</b>	IAT II	PMP and/or CAPM	Experience providing theater level Mission Command (MC)/Command and Control (C2) systems engineering support in planning for future activities by developing support documents for the Contingency Operations (CONOPS), Operational Plans (OPLANS) and strategic plans
<b>iArmy / CMDWeb</b>	IAT II	Agile development (SCRUM and Ozone Widget Framework)	Experience installing, and managing development environments and modifying Java code for widgets developed within the Ozone Widget framework.
<b>Chief of Staff PROVOST MARSHAL OFFICE, IACS</b>			
<b>IACS Data Base Administrator (DBA) Counter Terrorism and Law Enforcement Data Analyst</b>	IAT II	Security+, Oracle Certified Professional (OCP) - Database Administrator (DBA) 11g	German language proficiency (written and oral) and Oracle DBA experience.
<b>IACS Biometric/Counter Terrorism Liaison Officer</b>	IAT II	Certified Biometrics Security Developer (CBSD)_	Experience in supporting DoD or industry equivalent biometric capabilities/programs
<b>HQ USAREUR G6</b>			
<b>TMT Support</b>	IAT II	CRM Certification	Experience in supporting the TMT application suite
<b>JMRC</b>			
<b>Frequency Management</b>	IAT II	CCNP and/or experience in Frequency Management	Experience in frequency management or documented formal training
<b>G6 CSD</b>			
<b>ACA Auditing</b>	IAM III	CISSP	Experience in performing ACA Auditing/Testing

## 10.2 INFORMATION ASSURANCE CONTRACTOR TRAINING AND CERTIFICATION

Pursuant to DFARS 252.239–7001 Information Assurance Contractor Training and Certification (JAN 2008):

- (a) The Contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01–M, Information Assurance Workforce Improvement Program. The Contractor shall meet the applicable information assurance certification requirements, including—
  - (1) DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01–M; and
  - (2) Appropriate operating system certification for information assurance technical positions as required by DoD 8570.01–M.
- (b) Upon request by the Government, the Contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions.
- (c) Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

Contractor personnel must agree as a "condition of employment" to obtain the appropriate baseline certification upon contract award. Contract employees shall maintain IA certification(s) appropriate to the individual's position in accordance with the guidance and procedures defined in DOD 8570.01-M. The IAM/IAT certification level required by the individual contractors shall be shown in the Contractor's Staffing Matrix.

IAW DoD 8570.01, Contractor personnel shall have an appropriate Computing Environment (CE) certification for the operating system(s) and/or security related tools/devices on which they will spend the majority of their time. The COR, in coordination with the QAE, will determine the appropriateness of the certifications which the contractor shall include the CE certification column in the Staffing Matrix. Industry credentials will change based on technology and Government changes. It is the contractor's responsibility to meet the 8570 Certification requirements at their own expense. The contractor shall collectively meet the desired CE Certification/Industry Credentials requirements for each Mission listed below.

PWS REF.	TASK AREA/FUNCTION	8570 CERTIFICATION REQUIREMENTS	DESIRED CE CERTIFICATION/DESIRED INDUSTRY CREDENTIAL
4.0	Program Management Office	IAT II	PMP
6.1	CHIEF OF STAFF KM	IAT II	CRM, Certified Knowledge Manager, or MCSD Certification
6.2	USAREUR G2	IAT II	CCNP, CCNA, ITIL, MCITP, CISSP
6.3	HQ G3 MCSD	IAT II	Solaris Certified System Administrator (SCSA), Red Hat Certified System Administrator (RHCSA), MCSA, MCSE, MCSA, MCP, VMWARE, Oracle Certified Associate (OCA), Oracle Certified Professional (OCP), CCNA-Routing & Switching (RS), CCNA-Security (SEC), JAVA, SCRUM, PMP, CISSP, CAPM
6.4	PROVOST MARSHAL OFFICE, IACS	IAT II	
	Project / Operational Management Support	IAT II	PMP, Security Plus, CE (Microsoft or CISCO), CCNA or MCSA
	IACS Database Administrator (DBA) Counter Terrorism and Law Enforcement Data Analyst/Liaison Support	IAT II	Security Plus, CE C, Oracle Certified Professional (OCP) - Database Administrator (DBA) 11g
	IACS Biometric/Counter Terrorism/Liaison Support	IAT II	Security Plus and CE, Certified Biometrics Security Developer (CBSD)
	Access Control Point Implementation and maintenance Support	IAT II	Security Plus, CE and CCENT or MCP Desktop
	IACS Network Engineer Support	IAT II	Security Plus, CE, CCNA, MCSA, VMWare Certified Professional

	IACS Installation Component Management Support	IAT II	Security Plus, CE and CCENT or MCP Desktop
	Continuity of Operations Documentation and Training Support	IAT II	SharePoint or CKM
6.5	USAREUR G6 HSD	IAT II	
	Software Engineering/Development Services	IAT II	MCTS: WSS, MCTS:MOSS, MCTS(CRM Platform): .Net Framework, Xamarin (mobile application), MCSE (Latest Windows Server version) , XML, MCSA, MCSD (SharePoint applications), ITIL
	System Engineering and Support Services	IAT II	MCITP (DBA/SQL), VMware CP, CCNP, RHCSA, Microsoft Lync Server
6.6	USAREUR G6 CyberSecurity	IAM III	CISSP, PMP
6.7	Joint Multinational Training Command G4	IAT II	CCNA or equivalent, ITIL
6.8	Joint Multinational Readiness Center S6	IAT II	
	Frequency Management	IAT II	Secret / SSBI
	(a) Help Desk Lead (b) Help Desk	IAT II	(a) MCSA (b) CCENT or MCP\MCTS Windows 7 or 8
	Network Management Support - JMRC	IAT II	CCNP:Wireless, CCNP:VOIP
	System Management Support	IAT II	MCSE, VMWare VCP
	Information Assurance Support	IAT III	CISSP or CASP, Enterprise Mission Assurance Support Service (eMASS) Risk Management Framework (RMF) Trained;
	Operations and Maintenance Services - MRX	IAT II	MCSA, CEH, MSCD or MCSM, NE2S proficient & Trained
	Systems Engineering	IAT III	PMP, CISSP or CASP, MCITP or MCSE, MCDBA
	VTC Systems Administration	IAT II	CCENT or MCP/MCTS Windows 7 or 8
6.9	European Theater PKI Services	IAT II	Acquire CNSS LRA and CNSS RA in 6mo (Government provided), MCP, Security+
6.10	AFRICOM CoS (Optional)	IAT II	SharePoint, Security+
6.11	AFRICOM J1 J8	IAT II	MCP, MCSE, SharePoint
6.12	AFRICOM J2	IAT II	CCNP, CCNA, ITIL, MCITP
6.13	409 <sup>th</sup> Contracting Support Brigade (Optional)	IAT II	MCP, MCSE, SharePoint
6.14	7 <sup>th</sup> Mission Support Command	IAT II	MCP, MCSE, SharePoint, CCNA, VMWare



6.15	EUCOM SGS TMT	IAT II	CRM, MCSD
6.16	21 <sup>st</sup> TSC (Optional)	IAT II	SharePoint, Security+
6.17	IMCOM-E USAG Italy	IAT II, IAM III	CISSP, CCNA or equivalent
6.18	5 <sup>th</sup> Signal Command (Optional)	IAT II	CCNA or equivalent
6.19	IMCOM-E USAG RP	IAT II	CCNA, MCP, SharePoint
6.VEN.1	Cisco Support Services	IAT II	CCIE
6.VEN.2	EMC Support Services	IAT II	EMCIE
6.VEN.3	MS Support Services	IAT II	MCP
6.VEN.4	NetApp Support Services	IAT II	NCIE
6.VEN	Other Vendor Support	IAT II	TBD
6.OPT	Optional Support Services	IAT II	Applicable Vendor Certification
<b>Note: IA Workforce certification requirements for the optional areas will be identified when exercised</b>			

## 11.0 ADMINISTRATIVE CONSIDERATIONS

### 11.1 POINTS OF CONTACT

The USAREUR COR, as defined by DFARS 201.602-2, is responsible for technical oversight of the Task Order and shall coordinate administration of this task order with the GSA COR. The GSA COR and USAREUR COR will monitor delivery and performance at the task order level. The Government anticipates using Quality Assurance Evaluators (QAE) to assist the USAREUR COR and GSA COR in monitoring performance. The USAREUR COR and QAEs will have on record at each location, a letter of designation, which outlines their responsibilities and duties required to support the Contracting Officer. The letter of designation will also establish the limitations of the authority of the USAREUR COR and QAEs. The USAREUR COR and QAE will be identified to the Contractor personnel at each location and the duties, responsibilities, limitations of the USAREUR COR and QAE will be provided to the Contractor personnel.

#### 11.1.1 GSA Contracting Officer's Representative (COR)

Michael Baumann

Phone: (+49) 0611143-537-6292 OR (+1) 215-446-5852

DSN. 314-537-6292

Email: [michael.j.baumann19.civ@mail.mil](mailto:michael.j.baumann19.civ@mail.mil) OR [michael.baumann@gsa.gov](mailto:michael.baumann@gsa.gov)

#### 11.1.2 GSA Contracting Officer (CO)

Katrina Lloyd

Phone: 215-446-4898

Email: [Katrina.Lloyd@gsa.gov](mailto:Katrina.Lloyd@gsa.gov)

#### 11.1.3 GSA Contracts Specialist

Thomas McCarthy

Phone: 215-446-5808

Email: [thomas.mccarthy@gsa.gov](mailto:thomas.mccarthy@gsa.gov)

#### 11.1.4 USAREUR Contracting Officer's Representative (COR)

To be provided post award

#### **11.1.5 USAREUR QAE(s)**

The QAE for each mission will be designated upon award and managed by the GSA COR and USAREUR COR.

#### **11.2 PERIOD OF PERFORMANCE**

This task order consists of 12-month Base Period with one (1) subsequent 12-month option period, with an effective date, as follows:

- Transition/Base Period: 1 Feb 2016 through 31 Jan 2017, *(Note: It is anticipated that the Transition Period will be from 1 Feb 2016 through 4 Apr 2016 and fully operational performance under the base period would begin on 4 April 2016.)*
- Option Year 1: 1 Feb 2017 through 31 Jan 2018
- Option Year 2: 1 Feb 2018 through 31 Jan 2019
- Option Year 3: 1 Feb 2019 through 31 Jan 2020
- Option Year 4: 1 Feb 2020 through 31 Jan 2021

The Government may extend the term of this task order by written notice to the contractor within 15 days of the expiration of the existing period of performance provided that a preliminary notice of the Government's intent to extend is provided at least 30 days before the expiration of the task order. The preliminary notice does not commit the Government to an extension. If the Government exercises this option, the extended task order shall be considered to include this option clause. The Government shall have the unilateral right to exercise options periods.

#### **11.3 PLACE OF PERFORMANCE**

Reference Section 3.0.

#### **11.4 WORK HOURS**

In a garrison environment, the Contractor work hours will be set at five days a week, 8 hours a day, 40 hour work week.

During training exercises, the Contractor work hours will be set at 7 days a week, 12 hours a day, 84 hour work week.

During deployment periods, the Contractor work hours will be set at 7 days a week, 12 hours per day, 84 hour work week.

For Kosovo, the Contractor work hours will be set at 6 days a week, 10 hours per day, 60 hour work week. Other Direct Costs are allowable for this location.

The Government will pay additional hours beyond normal work hours on a straight time basis.

##### **11.4.1 SCHEDULING**

The Contractor shall schedule work hours that coincide with those of the supported activity. The Contractor shall coordinate the proposed work schedule with the COR or QAEs. Periodically, the Government will require Contractor support outside established duty hours. The Contractor shall ensure coverage during this entire period.

The COR may modify the work schedule to ensure the Government's ability to continue to execute its mission. Any modification to the Contractor's work schedule will have to be approved by the QAE/Contracting Officer in

writing and sufficient notice given to the Contractor, normally a minimum of one reporting period prior to the new work schedule (e.g. 1 month), for the Contractor to have ample time to make changes.

#### **11.4.2 ON-CALL SERVICE OR EXTENDED HOURS**

The Contractor shall be available to work “on-call” to ensure that mission essential equipment as designated by the site QAE/USAREUR COR is kept operational and is able to meet mission essential tasks as directed by the QAE/USAREUR COR.

The Contractor shall provide a 24-hour on-call roster to the QAE/COR for replication and distribution to assigned Government personnel. The initial on-call roster is due upon task order start date and shall be maintained throughout performance. Subsequent rosters are due a minimum of one week prior to expiration of the previous roster.

After Action Reports (AAR) shall be prepared in accordance with the Government provided AAR template for all after hours and overtime service requested and worked and forwarded to the respective QAE by the next business day. This shall include an update on the what, when, where, why, and how the problem/outage/corrections were made; impact on customers to include the length of time a problem existed; documentation of fix actions; and a way to ensure the problem does not recur.

#### **11.4.3 HOLIDAYS**

The following federal holidays are observed and therefore shall be staffed similar to other non-duty days (i.e. weekends):

- New Year Day
- Martin Luther King Day
- President’s Day
- Memorial Day
- Independence Day
- Labor Day
- Columbus Day
- Veteran’s Day
- Thanksgiving Day
- Christmas Day

#### **11.5 TRAVEL**

Contractor personnel are required to travel to work sites away from their primary sites in order to perform tasks during both peacetime and wartime periods in support of all software training, support and contingency operations as required. During wartime this may require travel to hostile war zones in support of systems. Authorized travel shall be payable as a direct cost. There will be no reimbursement for local travel for “in and around” mileage within a 50 mile radius of the Contractor’s official duty location.

The Government QAE must authorize all travel in advance. Air travel will be accomplished on regularly scheduled commercial flights using the most economical manner consistent with the successful accomplishment of the mission. Reimbursement for the cost of lodging and incidental expenses will be considered to be reasonable and allowable to the extent that costs submitted for reimbursement do not exceed the rates and amounts allowed by the Joint Travel Regulation as applies to civilian employees of the United States Government. Requests for movement by air will be submitted to the QAE/USAREUR COR at least 30 days prior to expected departure date.

#### **11.5.1 USE OF GOVERNMENT TRANSPORTATION**

The contractor is authorized to use available Government transportation services (Shuttle Buses) and operate and ride in vehicles (Transportation Motor Pool (TMP) to perform mission requirements (per FAR Clause 51.200 Contractor Use of Interagency Fleet Management System (IFMS) Vehicles). The contractor will be required to obtain necessary TMP licensing, training requirements and insurance to operate TMP vehicles. The usage and availability of Government transportation resources will be determined by individual site organizational policies. The site QAE will determine usage due to availability of government transportation resources. If Government transportation resources are available to meet mission requirements and the contractor chooses to another form of transportation, the government will not reimburse the contractor.

##### **11.5.1.2 TRAVEL REGULATIONS**

The Contractor shall adhere to the following travel regulations (see FAR 31.205-46):

- (1) Federal Travel Regulations (FTR) – prescribed by the General Services Administration, for travel in the contiguous United States.
- (2) Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, “Maximum Travel Per Diem Allowances for Foreign Areas”, prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

##### **11.5.1.3 TRAVEL AUTHORIZATION REQUESTS**

Before undertaking travel to any Government site or any other site in performance of this Task Order, the Contractor shall have this travel approved by, and coordinated with, the COR. The Contractor shall notify the COR prior to any anticipated travel. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long distance travel, the Contractor shall prepare a Travel Authorization Request for Government review and approval. The Government shall approve all travel in writing. Long distance travel will be reimbursed for cost of travel comparable with the FTR and DSSR.

Requests for travel approval shall:

- Be prepared in a legible manner;
- Include a description of the travel proposed including a statement as to purpose;
- Be summarized by traveler;
- Identify the travel request/travel authorization number associated with the travel;
- Be submitted in advance of the travel with sufficient time to permit review and approval.
- Not be considered approved until written approval is received from the COR (email shall suffice).

The Contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

##### **11.5.1.4 TRIP REPORTS**

The Government will identify the need for a Trip Report (if required) when the request for travel is submitted. The Contractor shall keep a summary of all long-distance travel, to include, at a minimum, the name of the employee, location of travel, duration of trip, and POC at travel location.

#### **11.6 NON-TRAVEL OTHER DIRECT COSTS (ODCs)**

##### **11.6.1 TOOLS**

The Government may require the Contractor to purchase hardware, software, and related items that are necessary and ancillary to the services being acquired under the TO. Such requirements will be identified at the time of award or may be identified during the course of a TO, by the Government or the Contractor. Tools purchased under this task order shall become the property of the government.

If the Contractor proposes the purchase of tools within the scope of a TO tasking, the Contractor shall submit to the Government COR a request to initiate purchase of such tools. The request shall include the purpose, specific items, estimated cost, cost comparison, and rationale. If approved and the task order is modified, the Contractor may proceed with the purchase. All purchases under this paragraph shall be made in accordance with the Federal Acquisition Regulation and the Contractor's Government approved purchasing procedures. All purchases shall be approved by the GSA COR in writing prior to execution. The Contractor shall categorize all procurements as either: (1) Mission Critical, (2) Urgent, or (3) Routine. The contractor shall notify (and, if necessary, request clarification from) the COR for all purchases requiring Mission Critical ordering.

If the Contractor initiates a purchase within the scope of this TO and the prime Contractor has an approved purchasing system, the Contractor shall submit to the COR a Request to Initiate Purchase (RIP). The RIP shall include the purpose, specific items, estimated cost, cost comparison to show competitive basis for fair and reasonable price determination, and rationale. The Contractor shall not make any purchases without a written approved RIP from the COR OR GSA CO. Email approvals are authorized.

In general, the Tools CLIN is anticipated for the purchase of IT assets or materials to update, maintain, establish or enable sustained C4I capabilities for the technical environments over the life of the Task Order. Purchases are expected to include, but are not limited to hardware and software, servers, network gear inclusive of switches, routers, NICs, hubs; laptops, desktops, handheld devices, storage devices and media; projectors, video telecom equipment, components, accessories, audio gear, displays, & related peripherals; VPN gear; miscellaneous peripherals, component parts & supplies, such as cables, couplers, connection kits; licensing and maintenance of operating system and application software products, security software and information assurance products; and related subscription-style technical and consultative-type services to enable productive deployment and efficient use of any hardware/software purchased and/or maintained under this TO.

The Contractor shall ensure that all communications and IT hardware provided has the most cost-effective warranty available from the vendor.

#### **11.6.2 OTHER DIRECT COSTS**

The Government may require the Contractor to incur ODCs incidental to performance under this task order. Such requirements will be identified at the time a TO is issued or may be identified during the course of a TO, by the Government or the Contractor. Reimbursement will be made as specified in the task order, consistent with the Alliant Contract.

Non-Travel ODC items (including tools) having a total procurement cost over \$3,000 per unit shall have the written approval of the USAREUR COR prior to procurement. Federal contracting laws and regulations apply to all Contractor open market purchases of materials and equipment under this task order. Prices must be determined fair and reasonable from competitive sources and are subject to Government audit. The Contractor shall maintain records documenting competitive sourcing, in strict compliance with the competition requirements set forth in the Federal Acquisition Regulation (FAR), for all material and ODC purchases. The Contractor shall provide copies of all such documentation upon request from the Government to verify that the Contractor complied with the competition requirements set forth in the FAR. Within the Contractor's price quote, any such rate shall be identified along with the DCAA point of contact (name, address, phone #, and email

address) for rate verification. The Contractor shall only be allowed to apply indirect rates to ODC costs after award if such application is consistent with their successful price proposal and DCAA recommendations. No profit or fee will be allowed on ODC costs.

All ODC items/materials purchased by the Contractor for the use or ownership of the Federal Government will become property of the Federal Government. If the Contractor acquires hardware/software maintenance support, all licenses and/or contractual rights to receive title shall be turned over to the Government upon completion of the task order. The Government's liability to reimburse the Contractor for costs incurred from the acquisition of hardware/software maintenance support shall be limited to costs incurred during the period of the order for which the Government received the said hardware/software maintenance support acquired by the Contractor on a cost reimbursable basis.

It is anticipated that miscellaneous ODCs necessary and incidental to performance may include but are not limited to:

- supplies, materials
- printing/copying costs; packaging & marking materials; shipping expenses
- logistical support

## **12.0 SPECIAL PROVISIONS UNDER THIS TASK ORDER**

### **12.1 AUTHORIZATION TO PERFORM SERVICES IN GERMANY**

Contractors performing services in the Federal Republic of Germany (FRG) shall comply with German law. The Contractor shall determine whether performance requires registration with German authorities or authorization to do business in Germany and, if so, shall comply with all requirements. Whether or not registration or authorization to do business is required, the Contractor also shall determine what documents or authorization its employees and any SubContractor employees must possess to work in Germany. The Contractor shall ensure affirmatively that its employees possess such documents or authorizations. Contractor employees who: (1) are not nationals of Germany or other European Union countries, and (2) are not members of the force, the civilian component or their dependents, and (3) do not have assimilated status under Articles 71, 72, or 73 of the Supplementary Agreement to the NATO SOFA shall possess work and residence permits.

By acceptance of and performance under this task order, the Contractor affirms that it has complied with the requirements above. Compliance with this clause and German law is a material contract requirement. Noncompliance by the Contractor or SubContractor at any tier shall be grounds for issuing a negative past performance evaluation and terminating this, task order for default.

#### **12.1.1 ADDITIONAL GUIDANCE FOR PERFORMANCE IN GERMANY**

Certain Contractor-owned or controlled structures and containers located on U.S. Government installations are subject to short-notice inspections by CFE treaty verification teams. The Government will endeavor to provide the Contractor as much notice as possible in the event of such inspections. The Contractor shall provide access to such structures and containers at the request of the Government and as soon as circumstances permit. The Contractor shall report such inspections to the Contracting Officer in writing within ten (10) calendar days of completion of the inspection. Contractor-owned or controlled structures and/or containers on U.S. installations may have to be inspected to comply with the CFE treaty even if Contractor personnel are unavailable to provide access. Any costs borne by the Contractor or any impact on contract performance as a result of the inspection will be a matter of negotiation between the Contractor and the Contracting Officer.



## **12.2 GENERAL THEATER REQUIREMENTS**

All DoD and DoD-sponsored personnel, including DoD-sponsored Contractors, will ensure personnel entrance requirements for country, theater, and/or special area clearance are met IAW Department of Defense Foreign Clearance Guide (DoD 4500.54-G)(FCG)<[www.fcg.pentagon.mil](http://www.fcg.pentagon.mil)> or classified supplement <[www.fcg.pentagon.smil.mil](http://www.fcg.pentagon.smil.mil)>. DoD-sponsored Contractors shall provide all required personnel data to the QAE

The Contractor shall ensure all deployed personnel are medically qualified to deploy and perform in austere environments where medical services are at a minimum. The Contractor shall provide approved deployment physical examination results for all personnel. The inability to comply with this requirement is grounds for dismissal.

## **13.0 GOVERNMENT FURNISHED RESOURCES**

### **13.1 FACILITIES**

The government will provide office facilities. The Contractor shall use Defense Service Network (DSN) to the maximum extent possible. The installation, maintenance, repair and removal of all Government furnished telephone/fax instruments will be the responsibility of the Government. The Contractor personnel shall not relocate the Government furnished telephone or fax equipment unless approved or directed by the functional area QAE. Unless otherwise noted, the Government will furnish essential day-to-day consumable operating supplies required for the performance of this task order.

The Contractor shall be responsible for keys and access cards provided by the Government. Keys will not be duplicated nor used by unauthorized personnel. The Contractor shall develop and implement procedures to ensure that keys issued to the Contractor are safeguarded and controlled in accordance with these regulations. Procedures implemented will be documented in the physical security plan. The government will furnish keys and locks required for the performance of the contract. The Contractor shall inventory all Government issued keys IAW with applicable guidance.

### **13.2 TRANSPORTATION**

As authorized by the Contracting Officer's Representative (with specific authority), Contractor Field Software Engineers (FSEs) and Digital Software Engineers (DSEs) may utilize military, leased or rented vehicles, in lieu of base shuttles, when necessary to provide timely software support to downrange military units supported by this task order.

### **13.3 FUEL**

In situations that dictate under this task order, fuel is authorized to be obtained from Government or military sources in accordance with processes defined by applicable regulation and policy with the supporting documentation and approval authorities required by Department of Defense, the United States Army and local Army commands.

### **13.4 GOVERNMENT FURNISHED PROPERTY (GFP) AND SERVICES**

- a. The Government will furnish the Contractor with technical manuals, supply catalogs, current software in support of this task order. Prior to any deployment, the Government may furnish specific equipment items, if available and necessary for that deployment.
- b. The Contractor is required to complete an inventory of Government-Furnished Equipment (GFE) i.a.w the milestones agreed to by the Government during the Transition-In at start of the contract, within 30 calendar days of the start of any option periods, and not later than 30 calendar days before completion of the task

order period. In the event of disagreement between the Contractor and the government representative on the working order and condition of equipment, the disagreement shall be treated as a dispute under the contract clause entitled "Disputes."

- c. The Government will provide DSL connectivity for the vendor Program Management office located within the Mission Command Center, Clay Kaserne, Wiesbaden, Germany as GFP.

### **13.5 LOGISTICAL SUPPORT AND PRIVILEGES IN HOST COUNTRY**

United States citizen Contractor employees who are authorized entry to the overseas command may be authorized by the discretion of local command policy, the Logistical Support Services defined in Appendix B, in accordance with DA PAM and AR 715-9.

### **13.6 GOVERNMENT FURNISHED LOGISTICS SUPPORT FOR DEPLOYED CONTRACTORS**

- a. The QAE at each site may identify certain equipment items as critical to mission operations. Systems using critical equipment must be returned to operational status within the times established by the QAE. If a critical equipment item spare is installed to replace a failed critical equipment item and installation of the spare returns the system to its full operational capability, then the critical equipment removed for repair shall be subject to the routine repair TAT. In no event shall the system be disrupted in excess of the time established for that particular system. Critical equipment shall be annotated as critical in the inventory management system.
- b. The Government shall provide field living conditions and amenities, equivalent to that available to military and/or Government civilians, to deployed contractor personnel.
- c. The Government is responsible for providing information on all requirements necessary for deployment.
- d. The COR will provide the contractor with the anticipated work schedule. The COR may alter the work schedule to ensure the Government's ability to continue to execute its mission. The COR will provide the contractor with the anticipated duration of the deployment.
- e. At no cost to the contractor, the Government will provide adequate force protection training for contractor personnel subject to deployment.
- f. The COR will inform the contractor of all Nuclear, Biological, and Chemical (NBC) equipment and Chemical Defensive Equipment (CDE) training requirements and standards.
- g. The Government shall provide the contractor employees with CDE familiarization training for the performance of mission essential tasks in designated high threat countries. This training shall be commensurate with the training provided to Department of Defense civilian employees.
- h. The COR shall identify to the contractor all identification cards and tags required for deployment and shall inform the contractor where the identification cards and tags are to be issued. Upon redeployment, the contractor shall ensure that all issued controlled identification cards and tags are returned to the Government.
- i. Unless authorized by the theater commander or his designee, contractors accompanying the force are not authorized to wear military uniforms, except for specific items required for safety and security. If required, the Government will provide the contractor all military unique organizational clothing and individual equipment. (Types of organizational clothing and individual equipment may include Nuclear, Biological, and Chemical defensive equipment and/or heavy winter clothing)

- j. The CO may direct the contractor, at the contractor's expense, to remove or replace any contractor employee failing to adhere to instructions and general orders issued by the COR. If a contractor employee departs an area of operations without permission, the contractor shall ensure continued performance in accordance with the terms and conditions of the contract. If the contractor replaces an employee who departs without permission, the replacement is at contractor expense and must be in place within five days or as directed by the CO.
- k. Contractor personnel may be authorized by the Government to travel in military vehicles.

### **13.7 CONTRACTOR FURNISHED LOGISTICAL SUPPORT FOR DEPLOYED CONTRACTORS**

- a. Contractor personnel subject to deployments shall have all passports, visas, and/or other documents, as well as inoculations necessary to enter and/or exit any area(s) identified by the COR. The contractor shall register all personnel with the appropriate US Embassy or Consulate.
- b. Contractor employees shall be subject to the customs processing procedures, laws, agreements, and duties of the country in which they are assigned to work and/or deploying to and the procedures, laws, and duties of the United States upon re-entry.
- c. When contractor personnel are required to deploy with users, contractor personnel shall perform under policies established by the Theater Commander. Contractor personnel shall meet theater personnel clearance requirements and obtain necessary personnel clearance prior to entering the AOR.
- d. In the event contractor personnel are not allowed to deploy to support a mission, contractor personnel will provide familiarization and instruction to Government personnel on basic maintenance techniques for the equipment items deployed. TAT for repair of any deployed equipment shall be on a "best effort" basis as dictated by the deployed operational environment.
- e. For equipment that may be deployed, as identified by COR, the contractor shall maintain a spares kit to ensure that adequate spare parts are available to support deployable equipment in the event of a training or crisis situation and to support all other deployments. The COR will authorize purchase of parts to support spares kits.
- f. The contractor shall brief employees regarding the potential danger, stress, physical hardships, and field living conditions that are possible if the employee deploys in support of military operations.
- g. The contractor, at no cost to the Government, may rotate contractor employees into and out of the theater provided there is no impact to the mission. The contractor shall coordinate personnel changes with the COR.
- h. At the request of the COR, the contractor shall report its employees, including third country nationals, entering, located within, and/or leaving the area of operations by name, citizenship, location, Social Security number (SSN), or other official identity document number. These reports shall be furnished to the COR at both the departing location and the receiving location.
- i. All deployed contractor employees and agents shall comply with pertinent Service and Department of Defense directives, policies, and procedures as provided by the COR. The contractor shall also ensure compliance with federal statutes, judicial interpretations, and international agreements (e.g., SOFAs, Host Nation Support Agreements, etc.) applicable to US Armed Forces or US citizens in the area of operations. Host Nation laws and existing SOFAs may take precedence over contract requirements.
- j. The contractor shall ensure that contractor employees possess the necessary and appropriate personal clothing and safety equipment to execute contract performance in the theater of operations in accordance

with the task order. Clothing should be distinctive and unique and not imply that the contractor is a military member, while at the same time not adversely affecting the Government's tactical position in the field.

- k. The contractor employee shall sign for all issued organizational clothing and individual equipment, thus, acknowledging receipt and acceptance of responsibility for the proper maintenance and accountability of issued organizational clothing and individual equipment. Upon completion of the deployment, the contractor shall ensure that all Government-issued clothing and equipment provided to contractor personnel is returned to the Government issuing office.
- l. Upon notification by the COR, the CO will require the contractor to reimburse the Government for organizational clothing and individual equipment lost or damaged due to contractor negligence.
- m. The contractor shall ensure that health and life insurance benefits provided to its deploying employees are in effect in the theater of operations. Insurance is available under the Defense Base Act and Longshoreman's and Harbor Workers Compensation Act administered by the Department of Labor or through self-insurance programs that provide similar coverage. The Government agrees to reimburse the contractor when in a hazardous duty state or hostile area. The reimbursement rate of pay is only authorized when deployed to a hazardous duty area, defined by the Government through State Department designations as appropriate.
- n. Before deployment, the contractor shall ensure that each contractor employee completes a DD Form 93, Record of Emergency Data Card, and returns the completed form to the COR.
- o. The contractor shall provide employees who are medically fit and capable of enduring the rigors of deployment in the designated theater of operations. Contractor personnel may be required to undergo medical screening, which may include DNA sampling. Medical screening requirements will be detailed by the host site. Any personnel deemed unsuitable to deploy during the deployment process, due to medical or dental reasons, will not be authorized to deploy with the military force.
- p. Deploying civilian contractor personnel shall carry with them a minimum of a 90-day supply of any medication they require.
- q. The contractor shall perform the requirements of this contract notwithstanding the fitness for duty of deployed employees, the provisions for care offered under this section, and redeployment of individuals determined to be unfit.
- r. The contractor bears the responsibility for ensuring all employees are aware of the conditions and medical treatment available at the performance location. The contractor shall include this information and requirement in all subcontracts with performance in the theater of operations.
- s. Whether contractor personnel will be permitted to carry a government furnished weapon for self-defense purposes in the Area of Operations (AO) is at the discretion of the Theater Commander. However, contractor personnel will not possess personally owned firearms in the AO. The government may choose to issue military-specification personal weapons and ammunition (M9 Pistols) for self-defense to the contractor employees. Acceptance of weapons by contractor employees is at the discretion of the Contractor and the contractor employees. When accepted, the contractor employee is responsible for using the weapon in accordance with the applicable rules governing the use of force. The contractor employee must be aware they may incur civil and criminal liability, both under host nation law or U.S. criminal and civil law, for improper or illegal use of the weapons. Also, only military issued ammunition may be used in the weapons.

#### **14.0 INVOICE SUBMISSION**

The Contractor shall submit Requests for Payments in accordance with the format contained in GSAM 552.232-70, INVOICE REQUIREMENTS (SEPT 1999), to be considered proper for payment. In addition, the data elements indicated below shall be included on each invoice.

Task Order number: *(from GSA Form 300, Block 2)*  
Paying Number: *(ACT/DAC NO.) (From GSA Form 300, Block 4)*  
Project No.  
Project Title

The Contractor shall provide invoice backup data in accordance with the contract type, including detail such as labor categories, rates and quantities of labor hours per labor category.

**Note:** The Government reserves the right to audit, thus; the Contractor shall keep on file all backup support documentation for Travel, Tools, and ODCs.

#### 14.1 INVOICE REQUIREMENTS

The Contractor shall submit a draft or advance copy of an invoice to the client POC for review prior to its submission to GSA as outlined in 14.2 Invoice Submission Process.

The contractor shall invoice monthly on the basis of cost incurred for the Labor, Base Fee, Travel, Tools, and ODC CLINs. The Period of Performance (POP) for each invoice *shall* be for one calendar month. The contractor *shall* submit only one invoice per month. The appropriate GSA office will receive the invoice by the twenty-fifth calendar day of the month after the end of the invoiced month.

**Content of Invoice:** The contractor's invoice shall be submitted monthly for work performed and/or costs incurred during the prior month. The contractor may invoice only for the hours, travel, tools, and ODCs, ordered by GSA and actually used in direct support of the client representative's project. To be considered proper, the invoice shall include the following information at a minimum:

- GSA Task Order Number *(from GSA Form 300, Block 2)*
- Gsa Task Order Paying Number: *(ACT/DAC NO.) (From GSA Form 300, Block 4)*
- ITSS Order ID No.
- Project Title
- Remittance Address
- Period of Performance for Billing Period
- Point of Contact and Phone Number
- Invoice Amount
- Travel and Training Itemized by Individual and Purpose (if applicable) billed to ODC CLIN
- Support Items listed by Specific Item and Amount (if applicable) billed to ODC or Tools CLIN as appropriate.

All hours and costs shall be reported by CLIN and shall be further subdivided to lower level WBS elements as directed by the Government to permit tracking and reporting of costs consistent with appropriation, regulatory, policy or other requirements. The contractor shall provide the invoice data in a Microsoft Excel spreadsheet in a format reviewed and approved by the Government. The Government reserves the right to modify invoicing requirements at its discretion. The contractor shall comply with any revised invoicing requirements at no additional cost to the Government.

**Final Invoice:** Invoices for final payment must be so identified and submitted within 6 months from task order completion. After this submission, no further charges are to be billed. A copy of the written client agency acceptance of task completion must be attached to final invoices. The contractor shall request from GSA an extension for final invoices that may exceed the 6-month time frame.

The Government reserves the right to require certification by a GSA COR before payment is processed, *if necessary*.

#### **14.1.1 COST PLUS FIXED FEE (CPFF) CLINS for LABOR**

The contractor shall invoice monthly on the basis of cost incurred for the CPFF Labor CLINs. All hours and costs shall be reported by CLIN element and contractor employee level, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data on separate worksheets in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

- Employee name (current and past employees)
- Employee company labor category
- Employee Alliant labor category
- Actual Hours worked during the monthly billing period and total cumulative hours worked
- Current costs billed and cumulative costs

All cost presentations provided by the contractor shall also include Overhead Charges, and General and Administrative Charges clearly shown both as a percentage and total dollars.

**Fixed Fee:** The contractor's monthly invoice shall include the current and cumulative Fixed Fee.

#### **14.1.2 TRAVEL**

The contractor shall adhere to FAR part 31.205-46 for travel associated with this contract. This shall include all travel requirements associated with temporary duty (TDY) or deployments as required under this task order, Contractor personnel are authorized to invoice travel related costs at the allowance referenced in FAR part 31.205-46.

Cost incurred for Travel shall be invoiced monthly with travel itemized by Individual and Trip. The contractor shall provide the Travel invoice data on separate worksheets in Microsoft Excel spreadsheet form with the following detailed information.

**CLIN Total Travel:** This invoice information shall identify all cumulative travel costs billed by CLIN. The current invoice period's travel detail shall include separate columns and totals and include the following:

- Travel Authorization Request Number or identifier
- Current invoice period
- Names of persons traveling
- Number of travel days
- Dates of travel
- Location of travel
- Number of days per diem charged
- Per diem rate used
- Total per diem charged



- Transportation costs
- Total charges

All cost presentations provided by the contractor shall also include Overhead Charges and General and Administrative Charges. Fee shall not be permitted on travel costs.

#### **14.1.3 TOOLS AND ODCs**

Cost incurred for the Tools and ODC CLINs shall be invoiced monthly. The contractor shall provide the Tools invoice data on separate worksheets in Microsoft Excel spreadsheet form with the following detailed information, as applicable.

- Tools purchased and/or ODC costs incurred
- Consent to Purchase Number or identifier
- Description of the Tools with the Quantity, Unit Price and Extended Price of each Tool and/or ODC identified
- Date accepted by the Government
- Associated CLINs
- Project to date totals by CLIN
- Cost incurred not billed
- Remaining funded balance of the associated CLINs

All cost presentations provided by the contractor shall also include Overhead Charges, General and Administrative Charges, and or material handling as appropriate and consistent with DCAA recommendations. Fee shall not be permitted on Tools and ODC costs.

#### **14.1.4 INDIRECT AND MATERIAL HANDLING RATE**

Travel, Tools, and ODC costs incurred may be burdened with the Contractor's indirect/material handling rate consistent with the contractor's cost proposal for this task order.

Any proposed indirect or material handling rates proposed and invoiced shall be consistent with the contractor's most recent Defense Contract Audit Agency (DCAA) rate approval, provisional rate letter or recommendations. Offerors are advised that they will not be permitted to apply a burden rate of any kind to travel, tools or ODC costs after award, except to the extent that application of such burden is consistent with their CAS Disclosure Statement, proposal practices, and the most current Defense Contract Audit Agency (DCAA)/ Defense Contract Management Activity (DCMA) recommendations. Cost Accounting Standards (CAS) are applicable in this procurement. Offerors shall propose in accordance with approved disclosure statement and established practices.

### **14.2 INVOICE SUBMISSION PROCESS**

#### **14.2.1 INVOICE PROCESS**

Invoice submission is a two-step process:

- a. Create an Invoice Acceptance Document in IT-Solutions Shop (ITSS).
- b. Obtain Client and GSA Acceptance.

To submit an invoice to ITSS for Client Acceptance, follow these steps:

1. Log onto the Internet URL <http://web1.itss.gsa.gov>.
2. Log into ITSS using your assigned username and password.
3. Once logged in, click on "Create Support Documents".
4. Once in the Create Support Documents field, you will see a list of awarded task order numbers and a pull down menu that reads <<Select Support Document>>. Select the appropriate task order number by highlighting it, then click on the pull down menu; select "Acceptance Information" and click on the "Create" icon.
5. You are now on the page where you will enter the delivery date and invoice number—do not use special characters in the invoice number and be sure to use exactly the same invoice number and value for GSA Finance. You have the opportunity to send comments to the client (receiving activity) in the detailed comments block. You must attach an electronic copy of your invoice. Click on the thumbtack "Attach" icon to bring up the attachments page. When you are done attaching the invoice, click on the "Submit" button at the bottom of the page to complete the process.

Note: By utilizing the submission methods described above, no paper copy of the invoice shall be submitted to GSA COR unless requested. The Contractor may be required to submit a written "hardcopy" invoice to the Government, or a hardcopy of the invoice with the client's certification if requested by the GSA COR.

When the Contractor's ITSS acceptance document is submitted, emails requesting Government acceptance are automatically sent to both the Client and the GSA Project Manager/COR. They will accept, partially accept, or reject the invoice, normally with explanatory comments. The Client will also indicate the amount approved for payment. The ITSS system will automatically notify you, the Vendor, of acceptance or rejection of the invoice.

If you need assistance or have any questions regarding the acceptance and approval process, please contact the ITSS Help Desk at the toll free number 1-877-243-2889. Be sure to have the ITSS Order number or ACT number available.

#### **14.2.2 INVOICE CLAUSE**

The Period of Performance (POP) for each invoice *shall* be for one calendar month. The contractor *shall* submit only one invoice per month per order/contract. The appropriate GSA office will receive the invoice by the twenty-fifth calendar day of the month after either:

- (1) The end of the invoiced month (*for services*) or
- (2) The end of the month in which the products (*commodities*) or deliverables (fixed-priced services) were delivered and accepted by the Government.

For Labor Hour and Time and Material orders/contracts each invoice shall show, the skill level category, the hours worked per skill level, the rate per skill level and the extended amount for that invoice period. It *shall* also show the total cumulative hours worked (inclusive of the current invoice period) per skill level, the hourly rate per skill level, the total cost per skill level, the total travel costs incurred and invoiced, and the total of any other costs incurred and invoiced, *as well as* the grand total of all costs incurred and invoiced.

For Labor Hour and Time and Material orders/contracts each invoice *shall clearly indicate* both the current invoice's monthly "burn rate" and the total average monthly "burn rate".

The contractor *shall submit* all required documentation (unless exempted by the contract or order) as follows:

For Travel: Submit the traveler's name, dates of travel, location of travel, and dollar amount of travel.

For ODCs: Submit a description of the ODC, quantity, unit price and total price of each ODC.

**Note**: The Government reserves the right to audit, thus; the contractor shall keep on file all backup support documentation for travel and ODCs.

**Note**: For Firm Fixed Price, Labor Hour, and Time and Material fiscal task items:

Charges:

- All invoice charges must be task item specific (only one task item) unless concurrent task item periods of performance exist.
- For invoices with concurrent task item periods of performance all invoice charges must be service month specific (that is one service month only).

Credits:

- If the credit invoice is for the same year of a particular ACT#, the contractor shall include that credit on a subsequent invoice submission against that same ACT#. If the contractor is unwilling to offset a subsequent invoice then they must submit a refund check.
- When the credit invoice is for a different year, the contractor shall submit a refund check for that credit invoice.

Invoices that net to a credit balance **SHALL NOT** be accepted. Instead a refund check must be submitted by the contractor to GSA accordingly. The refund check shall cite the ACT Number and the period to which the credit pertains. The contractor shall provide the credit invoice as backup documentation. Do not attach credit invoice in ITSS or on the Finance website. It must be attached to the refund check. The refund check shall be mailed to:

General Services Administration  
Finance Division  
P.O. Box 71365  
Philadelphia, PA 19176-1365

**Posting Acceptance Documents**: Invoices shall be submitted monthly through GSA's electronic Web-Based Order Processing System, currently ITSS to allow the client and GSA COR to electronically accept and certify services received by the customer representative (CR). Included with the invoice will be all back-up documentation required such as, but not limited to, travel authorizations and training authorizations (including invoices for such).

**Receiving Agency's Acceptance**: The receiving agency has the following option in accepting and certifying services:

- a. Electronically: The client agency may accept and certify services electronically via GSA's electronic Web-Based Order Processing System, currently ITSS, by accepting the Acceptance Document generated by the contractor. Electronic acceptance of the invoice by the CR is considered concurrence and acceptance of services.

Electronic acceptance of the invoice by the CR is considered concurrence and acceptance of services. The contractor shall seek acceptance and electronically post the acceptance document in GSA's electronic Web-based Order Processing System, currently ITSS. After acceptance of the invoice by the CR, the Contractor shall submit a proper invoice to GSA Finance ([www.finance.gsa.gov/defaultexternal.asp](http://www.finance.gsa.gov/defaultexternal.asp)) not later than five (5) workdays after acceptance by the Government of the product, service, and/or cost item.

**Note:** The acceptance of the authorized agency customer representative is REQUIRED prior to the approval of payment for any invoiced submitted and shall be obtained prior to the approval of payment. In order to expedite payment, it is *strongly recommended* that the contractor continue to include the receiving agency's electronic acceptance of all the services or products delivered, with signature of the authorized agency customer representative and the date of acceptance, as part of the submission documentation.

**Note:** If *any* invoice is received without the required documentation and, the customer's electronic acceptance, the invoice *shall* be rejected in whole or in part as determined by the Government.

**Posting Invoice Documents:** Contractors shall submit invoices to GSA Finance for payment, after acceptance has been processed in GSA's electronic Web-Based Order Processing System, currently ITSS. The contractor is to post the invoice on GSA's Ft. Worth web site, [www.finance.gsa.gov/defaultexternal.asp](http://www.finance.gsa.gov/defaultexternal.asp)

**Content of Invoice:** The contractor's invoice will be submitted monthly for work performed the prior month. The contractor may invoice only for the hours, travel and unique services ordered by GSA and actually used in direct support of the client representative's project. The invoice shall be submitted on official letterhead and shall include the following information at a minimum.

1. GSA Task Order Number
2. Task Order ACT Number
3. Remittance Address
4. Period of Performance for Billing Period
5. Point of Contact and Phone Number
6. Invoice Amount
7. Skill Level Name and Associated Skill Level Number
8. Actual Hours Worked During the Billing Period
9. Travel Itemized by Individual and Trip (if applicable)
10. Training Itemized by Individual and Purpose (if applicable)
11. Support Items Itemized by Specific Item and Amount (if applicable)

**Final Invoice:** Invoices for final payment must be so identified and submitted within 60 days from task completion and no further charges are to be billed. A copy of the written acceptance of task completion must be attached to final invoices. The contractor shall request from GSA an extension for final invoices that may exceed the 60-day time frame.

The Government reserves the right to require certification by a GSA COR before payment is processed, *if necessary*.

#### **Close-out Procedures.**

**General:** The contractor shall submit a final invoice within sixty (60) calendar days after the end of the Performance Period. After the final invoice has been paid the contractor shall furnish a completed and signed

Release of Claims (GSA Form 1142) to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment.

## **15.0 PERSONNEL QUALIFICATIONS**

IAW DOD 8570.01-M entitled 'Information Assurance Workforce Improvement Program requires all individuals performing Information Assurance functions to be certified appropriate to the position. Information Assurance functions includes all personnel with "elevated privileges" on the network and personnel who perform IA management functions. DOD 8570.01-M further stipulates that "Contractor personnel...shall obtain the appropriate DoD-approved IA baseline certification, prior to being engaged. Contractors have up to 6 months to obtain the rest of the qualifications for their position". For the purpose of this contract "the rest of the qualifications" is defined as Computer Environment qualifications.

The Contractor shall maintain certification for all IA positions in accordance with DoD Regulation 8570.01M and adhere to the Army 8570 tracking process. The Contractor shall use ATCTS and other systems as designated by the Government to track contractor qualifications.

The Contractor shall clearly show the task area(s) supported and proposed certification level in their Staffing Matrix.

## **15.1 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS**

### **15.1.1 ORGANIZATIONAL CONFLICT OF INTEREST**

If the Contractor is currently providing support or anticipates providing support that creates or represents an actual or potential organizational conflict of interest (OCI), the Contractor shall immediately disclose this actual or potential OCI in accordance with FAR Subpart 9.5. The Contractor is also required to complete and sign an Organizational Conflict of Interest Statement in which the Contractor (and any SubContractors, consultants or teaming partners) agrees to disclose information concerning the actual or potential conflict with any proposal for any solicitation relating to any work in the TO. All actual or potential OCI situations shall be identified and addressed in accordance with FAR Subpart 9.5.

If a potential organizational conflict of interest is identified prior to award or during performance of this task order, the Contractor shall negotiate in good faith with the Government to resolve any such conflict or potential conflict pursuant to FAR 9.5 - Organizational and Consultant Conflicts of Interest.

The Contractor agrees that if it provides, under this Task Order, any systems engineering and technical guidance for systems and programs, but does not have overall contractual responsibility, it will not be allowed to be awarded a contract or task/delivery order to supply the system or any of its major components or be a sub-contract holder or consultant to a supplier of the system or any of its major components (FAR 9.505-1).

The Contractor agrees that if it assists in the preparation of non-developmental specifications or of work statements for a system or services under this Task Order, or assists in the development of acquisition strategies or evaluation criteria or otherwise provides acquisition support under this Task Order, it will not be allowed to furnish these items or services, either as a prime Contractor, a subcontract holder or as a consultant (FAR 9.505-2).

The Contractor agrees that if it gains access to proprietary data of other companies, it will protect such data and it will not use such proprietary data in supplying systems or components in future competitive procurements (FAR 9.505-4). In addition, the Contractor agrees to protect the proprietary data and rights of other organizations disclosed to the Contractor or Contractor's employees during performance of this Task Order with

the same caution that a reasonably prudent Contractor would use to safeguard highly valuable property. The Contractor also agrees that if it gains access to the proprietary information of other companies that it will enter into an agreement with the other companies to protect their information from unauthorized use or disclosure for as long as it remains proprietary and refrain from using the information for any purpose other than that for which it was furnished.

The Contractor agrees that it will not distribute reports, data or information of any nature arising from its performance under this Task Order, except as provided by this Task Order or as may be directed by the Contracting Officer.

The Contractor agrees that it will neither evaluate nor advise the Government with regard to its own products or activities. The Contractor shall objectively evaluate or advise the Government concerning products or activities of any prospective competitors.

The Contractor agrees that it will include the above provisions, including this paragraph, in agreements with teaming partners, consultants or subcontract holders at any tier that involve access to information covered above. The use of this clause in such agreements shall be read by substituting the word "teaming partner," "consultant," or "sub BPA holder" for the word "Contractor" whenever the latter appears.

#### **15.1.2 NON DISCLOSURE REQUIREMENTS**

All Contractor personnel (to include SubContractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the TO issued which requires the Contractor to act on behalf of, or provide advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, shall execute and submit an "Employee/Contractor Non-Disclosure Agreement" Form (Appendix G). See FAR 3.104, discussing requirements for disclosure, protection, and marking of Contractor bid or proposal information, or source selection information. All Contractor personnel must submit a Non-Disclosure Agreement prior to the commencement of any work on the task order. Further, Contractor personnel must submit a Non-Disclosure agreement whenever replacement personnel are proposed. Any information provided by Contractors in the performance of this TO or obtained by the Government is only to be used in the performance of the TO.

#### **15.2 CONTRACTOR'S PURCHASING SYSTEMS**

The objective of a Contractor purchasing system assessment is to evaluate the efficiency and effectiveness with which the Contractor spends Government funds and complies with Government policy with subcontracting.

As part of the evaluation for task order award, the Contracting Officer shall verify the validity of the Contractor's purchasing system. Thereafter, the Contractor is required to certify to the Contracting Officer no later than (30) days prior to the exercise of any options the validity of their purchasing system. Additionally, if reviews are conducted of the purchasing system after the exercise of the option, the Contractor shall provide the results of the review to the Contracting Officer within two weeks from the date the results are known to the Contractor.

#### **15.3 TRANSFER OF HARDWARE/SOFTWARE MAINTENANCE AGREEMENTS**

If the Contractor acquires hardware/software maintenance support, all licenses and/or contractual rights to receive title shall be turned over to the Government upon completion of the task order.

The Government's liability to reimburse the Contractor for costs incurred from the acquisition of hardware/software maintenance support shall be limited to costs incurred during the period of the order for which the Government received the hardware/software maintenance support acquired by the Contractor on a cost reimbursable, no fee basis.



## 16.0 CONTRACT CLAUSES

All applicable provisions and clauses shall flow down to subcontractors on this task order. (See PWS Sections 14.0 and 15.0).

NOTE: Section I of the Contractor's Basic Contract is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies and are incorporated by reference:

### 16.1 FEDERAL ACQUISITION REGULATION (FAR) CLAUSES

<u>CLAUSE NO.</u>	<u>CLAUSE TITLE</u>	<u>DATE</u>
SECTION 9.5	ORGANIZATIONAL CONFLICT OF INTEREST	
52.203-11	CERTIFICATION AND DISCLOSURE REGARDING PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS	(SEP 2007)
52.204-2	SECURITY REQUIREMENTS	(AUG 1996)
52.204-9	PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL	(JAN 2011)
52.215-21	REQUIREMENTS FOR COST OR PRICING DATA OR INFORMATION OTHER THAN COST OR PRICING DATA – MODIFICATIONS	(OCT 2010)
52.217-8	OPTION TO EXTEND SERVICES Fill-In Date: _30 days;_ 60 days; 60 months	(NOV 1999)
52.217-9	OPTION TO EXTEND THE TERM OF THE CONTRACT Fill in Dates: 30 days, 60 days.	(MAR 2000)
52.219-8	UTILIZATION OF SMALL BUSINESS CONCERNS	(JUL 2013)
52.222-25	AFFIRMATIVE ACTION COMPLIANCE	(APR 1984)
52.224-2	PRIVACY ACT NOTIFICATION	(APR 1984)
52.227-14	RIGHTS IN DATA- GENERAL	(DEC 2007)
52.227-21	TECHNICAL DATA DECLARATION REVISION AND WITHHOLDING OF PAYMENT – MAJOR SYSTEMS	(DEC 2007)
52.228-3	WORKERS COMPENSATION INSURANCE (DEFENSE BASE ACT)	(APRI 1984)
52.228-4	WORKERS COMPESATION AND WAR- HAZARDOUS INSURANCE OVERSEAS)	(APR 1984)
52.232-18	AVAILABILITY OF FUNDS	(APR 1984)
52.232-19	AVAILABILITY OF FUNDS FOR NEXT FY	(APR 1984)
52.232-2	LIMITATION OF COST	(APR 1984)
52.232-22	LIMITATION OF FUNDS	(APR 1984)
52.237-3	CONTINUITY OF SERVICES	(JAN 1991)
52.244-6	SUBCONTRACTS FOR COMMERCIAL ITEMS	(JUL 2013)
52.245-1	GOVERNMENT PROPERTY	(APR 2012)

52.251-1	AUTHORIZATION TO USE GOVERNMENT SUPPLY SOURCES	(APR 2012)
52.228-3	WORKERS COMPENSATION INSURANCE (DEFENSE BASE ACT)	(APR 1984)
52.222-54	EMPLOYMENT ELIGIBILITY VERIFICATION	(AUG 2013)
52.228-4	WORKERS COMPENSATION AND WAR - HAZARD INSURANCE OVERSEAS	(APR 1984)
52.217-5	EVALUATION OF OPTIONS	(JUL 1990)
52.245-1	GOVERNMENT PROPERTY	(JUN 2007)
52.237-3	CONTINUITY OF SERVICES	(JAN 1991)

## 16.2 DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT (DFARS) CLAUSES

<u>CLAUSE NO.</u>	<u>CLAUSE TITLE</u>	<u>DATE</u>
	CONTRACTOR MANPOWER REPORTING	
252.204-7004	ALTERNATE A CENTRAL CONTRACTOR REGISTRATION	(MAY 2013)
252.227-7013	RIGHTS IN TECHNICAL DATA - NONCOMMERCIAL ITEMS	(JUN 2013)
252.227-7014	RIGHTS IN NONCOMMERCIAL COMPUTER SOFTWARE AND NONCOMMERCIAL COMPUTER SOFTWARE DOCUMENTATION	(MAY 2013)
252.227-7015	TECHNICAL DATA- COMMERCIAL ITEMS	(JUN 2013)
252.227-7016	RIGHTS IN BID OR PROPOSAL INFORMATION	(JUN 2011)
252.227-7019	VALIDATION OF ASSERTED RESTRICTIONS - COMPUTER SOFTWARE	(SEP 2011)
252.227-7028	TECHNICAL DATA OR COMPUTER SOFTWARE PREVIOUSLY DELIVERED TO THE GOVERNMENT	(JUN 1995)
252.232-7007	LIMITATION OF GOVERNMENT'S OBLIGATION	(MAY 2006)
252.246-7001	WARRANTY OF DATA	(DEC 1991)
252.225-7043	ANTITERRORISM/FORCE PROTECTION FOR DEFENSE CONTRACTORS OUTSIDE THE UNITED STATES	(MAR 2006)
252.228-7003	CAPTURE AND DETENTION	(DEC 1991)
252.225-7040	CONTRACTOR PERSONNEL AUTHORIZED TO ACCOMPANY U.S. ARMED FORCES DEPLOYED OUTSIDE THE UNITED STATES	(FEB 2013)
252.239-7001	INFORMATION ASSURANCE CONTRACTOR TRAINING AND CERTIFICATION	(JAN 2008)

## 16.3 SECTION 508 COMPLIANCE

Unless the Government invokes an exemption, all EIT products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 CFR 1194. The Contractor shall identify all EIT products and services proposed, identify the technical standards applicable to all products and services proposed and state the degree of compliance with the applicable standards. Additionally, the Contractor must clearly indicate where the information pertaining to Section 508

compliance can be found (e.g., Vendor's or other exact web page location). The Contractor must ensure that the list is easily accessible by typical users beginning at time of award.

The Contractor must ensure that all EIT products and services proposed that are less than fully compliant, are offered pursuant to extensive market research, which ensures that they are the most compliant products available to satisfy the solicitation's requirements.

If any such EIT product or service proposed is not fully compliant with all of the standards, the Contractor shall specify each specific standard that is not met; provide a detailed description as to how the EIT product or service does not comply with the identified standard(s); and shall also indicate the degree of compliance.

## **17.0 APPENDICES**

- A. Sites and Customer Base
- B. Logistical Support Annex for European Theater
- C. Logistical Support Annex for Austere Locations
- D. Quality Assurance Surveillance Plan (QASP)
- E. Acronym Definition List
- F. DD Form 254 (To be provided post award)
- G. Contractor Employee Non-Disclosure Agreement (SAMPLE)
- H. Consolidated Hardware and Software List
- I. IACS USAREUR Network Topology Diagram
- J. JMRC VTC Equipment List
- K. USAREUR G2 Networks and Systems
- L. Performance Requirements Summary